ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

Τμήμα: Εφαρμογές Πληροφορικής στη Διοίκηση και στην Οικονομία

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κρυπτογραφία και ασφάλεια ηλεκτρονικού ταχυδρομείου: Το σύστημα PGP

Σπουδάστρια: ***Κουντούρη Πηνελόπη***

Επιβλέπων καθηγητής: ***Σιούτας Σπυρίδων***

Πρόλογος

Το τέλος του 20ου αιώνα χαρακτηρίζεται από την ανάπτυξη της κοινωνίας της πληροφορίας. Έτσι σήμερα είναι γεγονός ότι τα μέσα για τις περισσότερες δραστηριότητες μεταξύ των ανθρώπων είναι τα δίκτυα υπολογιστών. Το σύνολο των επικοινωνιών ανάμεσα σε εμπορικές και μη συναλλαγές παγκοσμίως εκτελείται από το μεγάλο επίτευγμα του διαδικτύου. Το βασικό του χαρακτηριστικό αποτελεί η ταχύτατη ανάπτυξή του και η μεγάλη του διεισδυτικότητα.

Συνέπεια αυτών είναι να εμφανίζεται το ζωτικό για την αποτελεσματικότητα του διαδικτύου πρόβλημα της ασφάλειας. Το πρόβλημα διογκώνεται λόγω των τεχνολογικών εξελίξεων και της αυτοματοποίησης των διαδικασιών. Ειδικότερα, ισχυρότεροι υπολογιστές και λογισμικό, ταχύτερα δίκτυα, έμπειροι χρήστες, αύξηση των διασυνδεδεμένων υπολογιστών αποτελούν απειλές για την ασφάλεια. Πριν από λίγα χρόνια, ένας κωδικός πρόσβασης επαρκούσε για ασφάλεια. Σήμερα η προσφερόμενη υπολογιστική ισχύς, η ταχύτητα επικοινωνίας και το εξειδικευμένο λογισμικό για παραβιάσεις, δημιουργεί ένα εντελώς ρευστό ως προς την ασφάλεια κατεστημένο επικοινωνιών.

Η πορεία ανάπτυξης των υπηρεσιών του διαδικτύου δεν συνοδεύτηκε από ανάλογη σε θέματα της ασφάλειας. Έτσι, χαλαρή διοίκηση/συντονισμός, τεχνολογική ετερογένεια, ανοικτό περιβάλλον λόγω παροχής πρόσβασης στο μεγαλύτερο αριθμό χρηστών κάνει την ίδια τη φύση του διαδικτύου να εμφανίζεται ως εχθρός της ασφάλειας.

Συγκεκριμένα, τα προβλήματα της ασφάλειας δικτύων χωρίζονται σε τέσσερις περιοχές:

1 *Μυστικότητα (secrecy):* είναι το πρόβλημα της παραβίασης πληροφοριών από μη-εξουσιοδοτημένους χρήστες.

2 *Πιστοποίηση αυθεντικότητας (authentication)*: Μιλάμε με αυτόν που νομίζουμε; Οι εισβολείς υποκρίνονται τον επιθυμητό παραλήπτη της επικοινωνίας μας.

3 *Μη απόρριψη υποχρέωσης ή οφειλής (non-repudation)*: Η περιοχή αυτή αποτελεί τις ψηφιακές υπογραφές προς απόδειξη πως συμφωνήθηκε κάτι και δεν μπορεί να ανακληθεί.

4 *Έλεγχος ακεραιότητας (integrity control)*: Επαλήθευση ότι το μήνυμα που λαμβάνεται είναι ίδιο με αυτό που στάλθηκε και δεν τροποποιήθηκε κατά την μετάδοση.

5 Η ασφάλεια επιτυγχάνεται με λύσεις σε καθένα από τα επίπεδα δικτύου:

6 *Φυσικό επίπεδο*: οι γραμμές μετάδοσης τοποθετούνται σε σφραγισμένους σωλήνες που περιέχουν αέριο σε υψηλή πίεση για ενεργοποίηση συναγερμού σε απόπειρα υποκλοπής.

7 *Επίπεδο σύνδεσης δεδομένων*: κωδικοποίηση στην αφετηρία, αποκωδικοποίηση στον προορισμό. Αυτό είναι προβληματικό όταν τα πακέτα διασχίζουν πολλούς δρομολογητές.

8 *Επίπεδο δικτύου*: φράγματα ασφαλείας (firewalls): συγκρατούν τα πακέτα μέσα ή έξω από μια περιοχή.

9 *Επίπεδο μεταφοράς*: κρυπτογράφηση συνδέσεων από άκρη σε άκρη, ή από διεργασία σε διεργασία.

Οι παραπάνω λύσεις αν και αντιμετωπίζουν αποτελεσματικά κάποια θέματα, δεν επαρκούν για πιστοποίηση αυθεντικότητας και μη-απόρριψη υποχρέωσης ή οφειλής. Αυτά αντιμετωπίζονται στο επίπεδο μεταφοράς. Τα παραπάνω προβλήματα καλείται να λύσει ο κλάδος της σύγχρονης κρυπτογραφίας. Από το πλήθος και τη βαρύτητα των προβλημάτων ασφαλείας συμπεραίνουμε πόσο δύσκολη γίνεται η ανάπτυξη λογισμικού για προστασία των δεδομένων του Η/Υ μας και ιδιαίτερα των

μηνυμάτων που ανταλλάσουμε στο διαδίκτυο χρησιμοποιώντας το ηλεκτρονικό ταχυδρομείο (e-mail). Την απάντηση σε αυτή την πρόκληση δίνει το σύστημα προστασίας δεδομένων PGP (Pretty Good Privacy). Είναι πολύ φιλικό στο χρήστη και παρέχει εκτός από προστασία μηνυμάτων ηλεκτρονικού ταχυδρομείου και πολλές άλλες δυνατότητες προστασίας δεδομένων.

Η πτυχιακή αυτή αποτελεί μια περιεκτική προσέγγιση των βασικότερων θεμάτων κρυπτογράφησης που αναφέρθηκαν πιο πάνω. Ξεκινώντας με μια ιστορική αναδρομή της κρυπτογραφίας από την αρχαιότητα εώς σήμερα, συνεχίζει με την περιγραφή βασικών μεθόδων κρυπτογράφησης και παρουσιάζει ενδιαφέρουσα και συμπαγή συλλογή αλγορίθμων που τις υλοποιούν. Επιπλέον, αναλύει θέματα ασφάλειας ηλεκτρονικού ταχυδρομείου, εστιάζοντας στο ευρέως διαδεδομένο συστήμα ασφάλειας ηλεκτρονικού ταχυδρομείου PGP, για το οποίο παρουσιάζει τις σχεδιαστικές του αρχές και τη βασική του δομή. Θεωρήθηκε σκόπιμο να συμπεριληφθεί στην πτυχιακή αυτή μέρος του εγχειρίδιου χρήσης του PGP. Αναλύονται οι βασικές οθόνες του, η δημιουργία των κλειδιών και οι εφαρμογές του στο ηλεκτρονικό ταχυδρομείο. Δεδομένης της μεγάλης εξάπλωσης του PGP, αναμένεται πως το εγχειρίδιο αυτό θα αποτελέσει χρήσιμο βοηθήμα στους αρχάριους του PGP.

Περιεχόμενα

Σχήματα

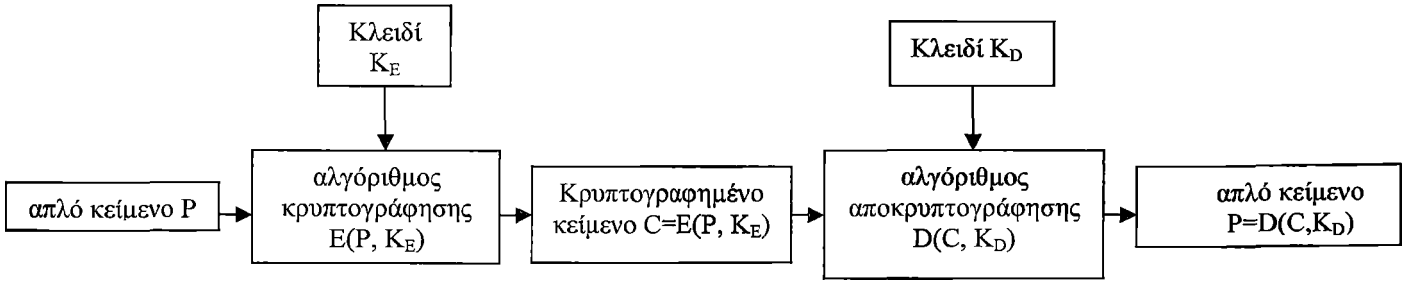
1 ΕΙΣΑΓΩΓΉ

1.1 Συστήματα Κρυπτογράφησης

Ο σκοπός της κρυπτογραφίας είναι να παραλάβει ένα μήνυμα ή αρχείο, που ονομάζεται απλό κείμενο (plain text), και να το αποκρυπτογραφήσει παράγοντας το κρυπτοκείμενο (ciphertext), με τέτοιο τρόπο ώστε μόνο εξουσιοδοτημένα άτομα να γνωρίζουν πως θα το μετατρέψουν αντίστροφα σε απλό κείμενο. Για όλους τους υπόλοιπους, το κρυπτοκείμενο είναι απλούστατα μια ακατονόητη σειρά από bits. Μπορεί να φαίνεται περίεργο στους αρχάριους, αλλά οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης (οι συναρτήσεις) πρέπει πάντα να είναι δημόσιες. Οι προσπάθειες απόκρυψής τους δε βοηθάει ποτέ και δίνει στους ανθρώπους που προσπαθούν να κρύψουν τα δεδομένα μια απατηλή αίσθηση ασφάλειας. Στο εμπόριο, η τακτική αυτή ονομάζεται ασφάλεια μέσω ασάφειας (security by obscurity) και εφαρμόζεται μόνο από ερασιτέχνες στην προστασία. Είναι αρκετά περίεργο το γεγονός ότι η κατηγορία αυτή περιλαμβάνει επίσης πολλές μεγάλες πολυεθνικές εταιρείες που θα έπρεπε να γνωρίζουν περισσότερα για το ζήτημα.

Αντίθετα η μυστικότητα εξαρτάται από παραμέτρους στους αλγόριθμους οι οποίες ονομάζονται κλειδιά (keys). Αν P είναι το αρχείο που περιέχει το απλό κείμενο, K_E είναι το κλειδί κρυπτογράφησης, C είναι το κρυπτοκείμενο και E ο αλγόριθμος κρυπτογράφησης (δηλαδή η συνάρτηση), τότε $C = E(P, K_E)$. Αυτός είναι ο ορισμός της κρυπτογράφησης. Δηλώνει ότι το κρυπτοκείμενο παράγεται με τη χρήση του (γνωστού) αλγόριθμου κρυπτογράφησης E, με παραμέτρους το απλό κείμενο P και το μυστικό κλειδί κρυπτογράφησης K_E.

Παρόμοια, ισχύει $P = D(C, K_D)$ όπου D είναι ο αλγόριθμος αποκρυπτογράφησης και K_D το κλειδί αποκρυπτογράφησης. Η σχέση αυτή δηλώνει ότι για να ληφθεί το απλό κείμενο P από το κρυπτοκείμενο C και το κλειδί αποκρυπτογράφησης K_D, ο χρήστης εκτελεί τον αλγόριθμο D με παραμέτρους τα C και K_D.



Σχήμα 1: Μέθοδος Κρυπτογράφησης και Αποκρυπτογράφησης

1.2 Εφαρμογές Συστημάτων Κρυπτογράφησης

Τα συστήματα κρυπτογράφησης τα συναντούμε στην καθημερινή μας ζωή σε μεγάλο πλήθος εφαρμογών. Μερικές από τις χρήσεις τους παρουσιάζονται στη συνέχεια.

1.2.1 Ασφαλής Επικοινωνία

Η ασφαλής επικοινωνία αποτελεί την πιο ευθεία χρήση της κρυπτογραφίας. Δύο άτομα μπορούν να επικοινωνήσουν με ασφάλεια με την κρυπτογράφηση των μηνυμάτων που ανταλλάσουν μεταξύ τους. Αυτό μπορεί να γίνει με τέτοιο τρόπο ώστε ένα τρίτο άτομο που παρακολουθεί τη συνομιλία να μην μπορεί ποτέ να αποκρυπτογραφήσει τα μηνύματα. Αν και το ζήτημα της ασφαλούς επικοινωνίας υφίσταται εδώ και αρκετούς αιώνες, το πρόβλημα της

διαχείρισης του κλειδιού ήταν αυτό που δρούσε ανασταλτικά. Χάρη στην ανάπτυξη κρυπτογραφίας δημοσίου κλειδιού, άτομα τα οποία μπορεί να μην γνωρίζονται μεταξύ τους έχουν πλέον την δυνατότητα επικοινωνίας με ασφάλεια.

1.2.2 Αναγνώριση, Πιστοποίηση και Εξουσιοδότηση

Ένα βασικό συστατικό στοιχείο ενός δικτύου είναι η ικανότητά του να αναγνωρίζει αξιόπιστα τους χρήστες. Η επίτευξη της αναγνώρισης (identification) συχνά βασίζεται στη χρήση ενός προσδιοριστικού (identifier, user id) που προσδιορίζει μονοσήμαντα ένα χρήστη και τον ξεχωρίζει από τους άλλους χρήστες του δικτύου.

Από τη στιγμή που ο χρήστης έχει αναγνωριστεί πρέπει να πιστοποιηθεί ότι είναι πράγματι αυτός που ισχυρίζεται πως είναι και όχι κάποιος άλλος που επιχειρεί να εξαπατήσει το σύστημα. Η διαδικασία αυτή ονομάζεται πιστοποίηση αυθεντικότητας ή απλά πιστοποίηση (authentication).

Αφού ο χρήστης έχει αναγνωριστεί και η ταυτότητά του έχει πιστοποιηθεί, τότε πρέπει να προσδιοριστούν τα δικαιώματα πρόσβασης του συγκεκριμένου χρήστη στο σύστημα. Η διαδικασία αυτή ονομάζεται εξουσιοδότηση (authorization).

1.2.3 Διαμοιρασμός Μυστικού (Secret Sharing)

Μια ακόμη εφαρμογή της κρυπτογραφίας αποτελεί ο λεγόμενος διαμοιρασμός μυστικού (secret sharing), το οποίο επιτρέπει το διαμοιρασμό μιας διαβαθμισμένης εμπιστευτικής πληροφορίας (ενός μυστικού), ανάμεσα σε μια ομάδα ατόμων, μέσα στην οποία υπάρχει προφανώς αμοιβαία εμπιστοσύνη. Η εφαρμογή αυτή χρησιμοποιεί συνήθως κρυπτογραφία ιδιωτικού κλειδιού. Παράδειγμα θα μπορούσε να αποτελέσει η διαδικασία όπου μικρές ομάδες ατόμων επικοινωνούν ιδιαιτέρως και συναποφασίζουν ποιο ιδιωτικό κλειδί θα χρησιμοποιούν. Επίσης, μια άλλη περίπτωση είναι επιχειρήσεις όπου μια διοικητική υπηρεσία γνωρίζει και διαχειρίζεται όλα τα κλειδιά. Τέτοιου είδους παραδείγματα αποτελούν τα κλειστά τραπεζικά συστήματα.

1.2.4 Ηλεκτρονικό Εμπόριο (E-commerce)

Τα τελευταία χρόνια όλο και μεγαλύτερος αριθμός εμπορικών συναλλαγών γίνεται μέσω του διαδικτύου (Internet). Η δραστηριότητα αυτή είναι γνωστή ως ηλεκτρονικό εμπόριο. Το ηλεκτρονικό εμπόριο, ανάμεσα στα άλλα, περιλαμβάνει τραπεζικές εργασίες πραγματικού χρόνου (online banking), χρηματιστηριακές συναλλαγές, αγορά και πώληση αγαθών μέσω του διαδικτύου. Κάθε καταναλωτής χρησιμοποιώντας την πιστωτική του κάρτα, μπορεί για παράδειγμα να αγοράσει ένα βιβλίο, να κάνει κράτηση αεροπορικών εισιτηρίων, να νοικιάσει αυτοκίνητο, να κλείσει δωμάτια σε ξενοδοχεία ενώ κάθεται δίπλα στον υπολογιστή του (ή απλά χρησιμοποιώντας το κινητό του τηλέφωνο στο λεγόμενο M-commerce).

Για να αντιμετωπίσει το φαινόμενο της απάτης ή/και της υποκλοπής των αριθμών των πιστωτικών καρτών χρησιμοποιούμε την κρυπτογραφία. Πιο συγκεκριμένα, κωδικοποιείται είτε ο αριθμός της πιστωτικής κάρτας είτε και ολόκληρη η διαδικασία της συναλλαγής. Όταν μια τερματική διάταξη κρυπτογραφεί τη συναλλαγή και τη μεταβιβάζει κωδικοποιημένα μέσω του διαδικτύου, αυτή είναι μη κατανοητή σε οποιοδήποτε άτομο που προσπαθεί να την υποκλέψει σε οποιαδήποτε φάση της επικοινωνίας. Για παράδειγμα, ο εξυπηρέτης (web server) λαμβάνει τα κρυπτογραφημένα δεδομένα, τα αποκρυπτογραφεί και προχωρεί στη συναλλαγή εξασφαλίζοντας μεταξύ των άλλων, ότι ο αριθμός της πιστωτικής κάρτας δεν έχει υποκλαπεί. Είναι προφανές ότι η αύξηση του όγκου των δοσοληψιών μέσω διαδικτύου οδηγεί σε ανάλογη αύξηση των απαιτήσεων ασφαλείας, προκειμένου να αντιμετωπιστούν απόπειρες «ηλεκτρονικής απάτης».

1.2.5 Πιστοποίηση/Έκδοση Βεβαίωσης

Μια ακόμη εφαρμογή αποτελεί και η «βεβαίωση». Η βεβαίωση αποτελεί ένα σχήμα σύμφωνα με το οποίο έμπιστοι αντιπρόσωποι, όπως είναι οι αρχές πιστοποίησης, βεβαιώνουν

την αυθεντικότητα αγνώστων αντιπροσώπων, ώστε αυτοί να θεωρούνται πλέον ως πιστοποιημένοι χρήστες. Η παραπάνω διαδικασία στηρίζεται στην έκδοση πιστοποιητικών από την πλευρά των έμπιστων αντιπροσώπων. Η συγκεκριμένη τεχνική αναπτύχθηκε με στόχο να καταστεί δυνατή η διαδικασία της αναγνώρισης και πιστοποίησης σε μεγάλη κλίμακα.

1.2.6 Ανάκτηση Κλειδιού

Η ανάκτηση κλειδιού είναι μια τεχνική σύμφωνα με την οποία ένα κλειδί γίνεται γνωστό, κάτω από ορισμένες συνθήκες, χωρίς ο ιδιοκτήτης του κλειδιού να το αποκαλύψει ο ίδιος. Η διαδικασία αυτή είναι χρήσιμη σε περιπτώσεις απώλειας του κλειδιού από το νόμιμο κάτοχό του ή σε περιπτώσεις παράνομων δραστηριοτήτων με στόχο τον εντοπισμό του δράστη.

1.2.7 Απομακρυσμένη Πρόσβαση

Η ασφαλής απομακρυσμένη πρόσβαση αποτελεί μια ακόμη εφαρμογή της κρυπτογραφίας. Το βασικό σύστημα πιστοποίησης μέσω των κωδικών (συνθημάτων), προσφέρει ένα επίπεδο ασφαλούς πρόσβασης. Και στην περίπτωση αυτή υπάρχει ωστόσο το ενδεχόμενο απώλειας ή κλοπής. Σήμερα, υπάρχουν πολλά προϊόντα που προσφέρουν κρυπτογραφικές μεθόδους για ασφαλή απομακρυσμένη πρόσβαση με υψηλότατο βαθμό ασφαλείας.

1.3 Ιστορικά Στοιχεία

Στην ενότητα αυτή κάνουμε μια σύντομη αναδρομή στην ιστορία της κρυπτογραφίας. Το υλικό που παρουσιάζεται εδώ αναφέρεται στις [Cohen95, Singh, Aegean].

1.3.1 Αρχαιότητα

Οι αρχαίοι **Κινέζοι** χρησιμοποιούσαν την ιδεογραφική φύση της γλώσσας τους, για να κρύψουν τα νοήματα των λέξεων. Τα μηνύματα συνήθως τα μετέτρεπαν σε ιδεογράμματα για ασφάλεια, αλλά δεν παρατηρείται σημαντική χρήση στα πρώτα χρόνια των Κινεζικών στρατιωτικών κατακτήσεων. Ο Τζένκινς Χαν για παράδειγμα, φαίνεται πως ποτέ δεν χρησιμοποίησε την κρυπτογραφία.

Στην **Ινδία** η μυστική γραφή ήταν εμφανώς πιο αποτελεσματική και η κυβέρνηση χρησιμοποίησε μυστικούς κωδικούς για να επικοινωνήσει με ένα δίκτυο κατασκόπων της, σκορπισμένων σε όλη τη χώρα. Οι πρωτοπόροι Ινδοί κρυπτογράφοι αναφέρθηκαν κυρίως σε απλά αλφαβητικά υποκατάστατα συχνά βασιζόμενα σε φωνητικά. Μερικά από αυτά ομιλούνταν ή χρησιμοποιούνταν ως απλή γλώσσα. Αυτό είναι παρόμοιο με το "pig latin" (igplay atinlay) όπου το πρώτο σύμφωνο τοποθετείται στο τέλος της λέξης και ακολουθείται από τον ήχο "ay".

Η κρυπτογραφική ιστορία της **Μεσοποταμίας** είναι παρόμοια με αυτή της **Αιγύπτου** στην οποία η σφηνοειδής γραφή χρησιμοποιείται εντός του κρυπτογραφημένου κειμένου. Αυτή η τεχνική είχε επίσης χρησιμοποιηθεί στη **Βαβυλώνα** και την **Ασσυρία**. Στη **Βίβλο**, μία εβραϊκή κρυπτογραφική μέθοδος εφαρμόστηκε κατά καιρούς. Σε αυτή τη μέθοδο, το τελευταίο γράμμα της αλφαβήτου αντικαθίσταται από το πρώτο, και αντίστροφα. Αυτό ονομάζεται "atbash". Για παράδειγμα ο ακόλουθος πίνακας δίνει μία ερμηνεία αυτής της μεθόδου για το αγγλικό αλφάβητο. Η λέξη "HELLO" γίνεται "SVOOL". Αν προσπαθήσουμε να αποκρυπτογραφήσουμε τη λέξη "WVXIBKG" τότε θα πάρουμε "DECRYPT".

απλό κείμενο	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
κρυπτογραφημένο	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Σχήμα 2: Μέθοδος Atbash

Στο περίφημο ομηρικό έπος της **Ιλιάδας**, η κρυπτογραφία χρησιμοποιήθηκε όταν ο Βελλεροφώντης διατάχθηκε να στείλει στο βασιλιά μια μυστική ταμπέλα, η οποία προέτρεπε το βασιλιά να σκοτώσει τον Βελλερεφώντη. Ο βασιλιάς προσπάθησε να τον σκοτώσει, στέλνοντάς τον να πολεμήσει σε αρκετές μυθικές μάχες αλλά αυτός νικούσε σε όλες!

Οι **Σπαρτιάτες** χρησιμοποίησαν ένα σύστημα το οποίο αποτελείτο από ένα λεπτό φύλλο παπύρου τυλιγμένο γύρω από μια ράβδο. Τα μηνύματα καταγράφονταν κατά μήκος της ράβδου και ο πάπυρος ξετύλιγε. Η διαδικασία της ανάγνωσης του μηνύματος, ήταν να τυλιχτεί ο πάπυρος γύρω από μια ράβδο ίσης διαμέτρου. Αυτό ονομαζόταν «κρυπτογράφημα σκυτάλης» και χρησιμοποιήθηκε κατά τους Πελοποννησιακούς πολέμους τον 5° αιώνα π.Χ. Χωρίς την κατάλληλη ράβδο ήταν δύσκολο να αποκωδικοποιηθούν τα μηνύματα χρησιμοποιώντας τις διαθέσιμες τεχνικές της εποχής. Η ακόλουθη διάταξη της αλφάβητου μας δείχνει πως λειτουργεί η τεχνική. Πρώτα θα δούμε την απόδοση του αλφαβήτου κατά το τύλιγμα και μετά κατά το ξετύλιγμα.

ADGJMP SVY
BEHKNQTWZ
CF I LORUX

(α) *κατά το τύλιγμα*

ADGJMPSVYBEHKNQTWZCF I LORUX

(β) *κατά το ξετύλιγμα*

Σχήμα 3: Κρυπτογράφημα Σκυτάλης

Μια ακόμα Ελληνική μέθοδος είχε αναπτυχθεί από τον **Πολύβιο** (σήμερα ονομάζεται «τετράγωνο του Πολύβιου»). Τα γράμματα της αλφαβήτου θα έπρεπε να αναπτυχθούν μέσα σε ένα 5x5 πίνακα. Οι γραμμές και οι στήλες είναι αριθμημένες από 1 ως 5 έτσι ώστε κάθε γράμμα να έχει ένα αντίστοιχο ζεύγος (γραμμής, στήλης). Αυτά τα ζεύγη θα μπορούσαν εύκολα να μεταδοθούν μέσω σημάτων καπνού ή με κινήσεις του χεριού. Η αποκρυπτογράφηση υπάρχει στην αντιστοιχία του ζεύγους των ψηφίων με τους αντίστοιχους χαρακτήρες τους. Αυτό το σύστημα ήταν το πρώτο που μείωνε το μέγεθος του συνόλου των συμβόλων και θα μπορούσε να χαρακτηριστεί ο πρόδρομος της σύγχρονης δυαδικής αναπαράστασης των χαρακτήρων. Ας προσπαθήσουμε να αποκωδικοποιήσουμε (Σχήμα 4/β) σύμφωνα με τον πίνακα του Πολύβιου (Σχήμα 4/α) το ακόλουθο μήνυμα (Σχήμα 4/γ).

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

(α) πίνακας του Πολύβιου

Π=14
Ι=42
Ν=33
Α=11
Κ=52
Α=11
Σ=34

Π=14
Ο=53
Λ= 13
Υ=54
Β=21
Ι=42
Ο=53
Υ=54

(β) αναπαράσταση χαρακτήρων

14423311521134
1453135421425354

(γ) κρυπτογραφημένο κείμενο

Σχήμα 4: Μέθοδος Πολύβιου

Ο **Ιούλιος Καίσαρας** χρησιμοποίησε ένα σύστημα της κρυπτογραφίας το οποίο μετατόπιζε κυκλικά 2 θέσεις δεξιά κάθε γράμμα του αλφαβήτου (π.χ. το Ψ μετατοπίζεται σε Α, το Ρ μετατοπίζεται σε Τ, κ.τ.λ.). Στο παρακάτω σχήμα, η πρώτη γραμμή απεικονίζει το απλό κείμενο, ενώ η δεύτερη γραμμή είναι η αντίστοιχη κρυπτογραφημένη. Η γενική περίπτωση αυτού του τμήματος του κρυπτογραφήματος είναι το «κρυπτογράφημα μονοαλφαβητικής αντικατάστασης» στο οποίο κάθε γράμμα μετατρέπεται σε άλλο γράμμα με μία «ένα προς ένα» αντιστοιχία. Ας προσπαθήσουμε να αποκωδικοποιήσουμε την κρυπτογραφημένη λέξη "EGCUCP". Θα προκύψει η λέξη: CEASAR

Απλό Κείμενο	**A**	B	**C**	D	**E**	F	G	H	J	K	L	M	N	O	P	Q	**R**	**S**	T	U	V	W	X	Y	Z
Κρυπτογραφημένο κείμενο	**C**	D	**E**	F	**G**	H	J	K	L	M	N	O	P	Q	R	S	**T**	**U**	V	W	X	Y	Z	A	B

Σχήμα 5: Μέθοδος Ιούλιου Καίσαρα

Η **κρυπτανάλυση** είναι η πρακτική της μετατροπής του κρυπτογραφημένου κειμένου σε απλό αναγνώσιμο, χωρίς πλήρη γνώση του κρυπτογραφήματος. Οι **Άραβες** ήταν οι πρώτοι που έκαναν σημαντικά άλματα στην κρυπτανάλυση. Ένας Άραβας συγγραφέας, ο Qalqashandi, έγραψε μία τεχνική για επίλυση κρυπτογραφημάτων η οποία χρησιμοποιείται ακόμα και σήμερα. Η τεχνική αυτή είναι η καταγραφή όλων των γραμμάτων του κρυπτογραφήματος και μέτρηση της συχνότητας του κάθε συμβόλου. Χρησιμοποιώντας το μέσο όρο της συχνότητας του κάθε γράμματος της συγκεκριμένης γλώσσας, μπορεί να εξαχθεί το πρωτότυπο κείμενο. Αυτή η τεχνική είναι ικανή να κρυπταναλύσει *κάθε* μονοαλφαβητικής αντικατάστασης κρυπτογράφημα, αν μας παρέχεται αρκετά μεγάλο τμήμα του κρυπτογραφημένου κειμένου. Η μέθοδος είναι γνωστή ως «συχνοτική ανάλυση».

1.3.2 Μεσαίωνας

Κατά τη διάρκεια του **μεσαίωνα**, η κρυπτογραφία ξεκίνησε να γνωρίζει ανάπτυξη. Όλες οι δυτικοευρωπαϊκές κυβερνήσεις χρησιμοποίησαν κρυπτογραφία διαφόρων τύπων και οι κώδικες άρχισαν να γίνονται όλο και πιο δημοφιλείς. Η κοινή χρήση των κρυπτογραφημάτων ήταν για να διατηρούν επαφή, οι κυβερνήσεις με τους απεσταλμένους τους. Οι πρώτες σημαντικές καινοτομίες στην κρυπτογραφία έγιναν στην **Ιταλία**. Στη Βενετία δημιουργήθηκε ένας πολυσύνθετος οργανισμός με μοναδικό σκοπό τις συναλλαγές με κρυπτογράφηση. Αυτοί είχαν τρεις γραμματείς-κρυπτογράφους, οι οποίοι έλυναν και δημιουργούσαν κρυπτογραφήματα που χρησιμοποιούνταν από την κυβέρνηση.

Ο Λέων Μπατίστα Αλμπέρτι ήταν γνωστός ως «ο πατέρας της δυτικής κρυπτολογίας» λόγω της ανάπτυξης από αυτόν της πολυαλφαβητικής αντικατάστασης. Η πολυαλφαβητική αντικατάσταση είναι κάθε τεχνική η οποία επιτρέπει διαφορετικά κρυπτογραφικά σύμβολα να παρουσιάζονται όμοια και ως σύμβολα απλού κειμένου. Αυτό κάνει πιο δύσκολη την ερμηνεία του κρυπτογραφήματος χρησιμοποιώντας συχνοτική ανάλυση. Στη συνέχεια, για να αναπτύξει αυτή την τεχνική, ο Αλμπέρτι ανέλυσε μεθόδους για σπάσιμο των κρυπτογραφημάτων και σχεδίασε ένα κρυπτογράφημα στο οποίο θα προσπαθούσε να καταστήσει αυτές τις τεχνικές άκυρες. Σχεδίασε δύο χάλκινους δίσκους προσαρμοσμένους ο ένας πάνω στον άλλον, ο κάθε ένας με το αλφάβητο χαραγμένο πάνω του. Για να ξεκινήσει η κρυπτογράφηση ενός προκαθορισμένου γράμματος πάνω στον εσωτερικό δίσκο, ευθυγραμμίζεται με ένα τυχαίο οποιοδήποτε γράμμα στον εξωτερικό δίσκο, το οποίο και γράφεται ως ο πρώτος χαρακτήρας του κρυπτογραφημένου κειμένου. Οι δίσκοι σταθεροποιούνται έτσι ώστε κάθε ένα από τα γράμματα του απλού κειμένου στον εσωτερικό δίσκο, να ευθυγραμμίζεται με ένα γράμμα από το κρυπτογραφημένο κείμενο επί του εξωτερικού δίσκου. Μετά από μερικές λέξεις, οι δίσκοι περιστρέφονται έτσι ώστε τα γράμματα του εσωτερικού δίσκου να ευθυγραμμίζονται με νέα γράμματα επί του εξωτερικού δίσκου και κατά αυτόν τον τρόπο το μήνυμα κωδικοποιείται. Περιστρέφοντας το δίσκο, μετά από κάποιο αριθμό λέξεων, το κρυπτογράφημα αλλάζει τόσο ώστε να περιορίσει την

αποτελεσματικότητα της συχνοτικής ανάλυσης. Αν και αυτή η τεχνική στη μορφή που την περιγράψαμε εμφανίζεται αρκετά ασθενής, η ιδέα της περιστροφής των δίσκων με αποτέλεσμα την αλλαγή του κρυπτογραφήματος, ήταν ένα μεγάλο επίτευγμα στην κρυπτογραφία.

Το επόμενο μεγάλο βήμα έγινε το 1518 από τον Τριθέμιο, έναν **Γερμανό** μοναχό που είχε ένα βαθύ ενδιαφέρον στο αντικείμενο. Έγραψε μία σειρά από 6 βιβλία με τίτλο "Πολυγραφία" και στο πέμπτο του βιβλίο κατασκεύασε έναν πίνακα που επαναλάμβανε το αλφάβητο της από πάνω σειράς, μετατοπισμένη κατά ένα γράμμα. Για την κωδικοποίηση ενός μηνύματος, το πρώτο γράμμα από το πρωτότυπο κείμενο κωδικοποιείται με την πρώτη γραμμή του πίνακα, το δεύτερο γράμμα με τη δεύτερη γραμμή του πίνακα κ.ο.κ. Αυτό παράγει ένα μήνυμα όπου όλα τα διαθέσιμα κρυπτογραφήματα χρησιμοποιούνται πριν επαναληφθούν. Στο Σχήμα 6 φαίνεται ένα εναλλασσόμενο κλειδί κρυπτογραφήματος αυτού του τύπου. Παρατηρούμε ότι η αντιστοίχιση των κωδικών συμβόλων με τα πρωτότυπα σύμβολα αλλάζει σε κάθε βήμα (K_0, K_1,.....K_{24}). Σε αυτό το σύστημα το κλειδί επαναλαμβάνεται κάθε 24 γράμματα κωδικοποιημένου κειμένου.

ΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩ --- απλό κείμενο

ΕΡΤΥΘΙΟΠΑΣΔΦΓΗΞΚΛΖΧΨΩΒΝΜ --- K_0

ΜΕΡΤΥΘΙΟΠΑΣΔΦΓΗΞΚΛΖΧΨΩΒΝ --- K_1

ΝΜΕΡΤΥΘΙΟΠΑΣΔΦΓΗΞΚΛΖΧΨΩΒ --- K_2

ΒΝΜΕΡΤΥΘΙΟΠΑΣΔΦΓΗΞΚΛΖΧΨΩ --- K_3

.....

ΡΤΥΘΙΟΠΑΣΔΦΓΗΞΚΛΖΧΨΩΒΝΜΕ --- K_{24}

Σχήμα 6: Κρυπτογράφημα εναλλασσόμενου κλειδιού

Το 1553, ο Γιοβάν Μπατίστα Μπελασό επέκτεινε αυτή την τεχνική επιλέγοντας μια λέξη κλειδί που είναι γραμμένη πάνω από το κείμενο, σε μία γράμμα προς γράμμα αντιστοίχιση. Η λέξη κλειδί επαναλειτουργεί με κάθε νέα λέξη απλού κειμένου. Το γράμμα της λέξης-κλειδί πάνω από το γράμμα του απλού κειμένου, είναι το πρώτο γράμμα της γραμμής του κρυπτογραφήματος που θα χρησιμοποιηθεί. Στις άλλες λέξεις, αν το γράμμα του πρωτότυπου κειμένου είναι 'β' και το γράμμα της λέξης-κλειδί είναι 'ρ', τότε η γραμμή του κρυπτογραφήματος του Τριθέμιου ξεκινά με το γράμμα 'ρ' να χρησιμοποιείται για να κρυπτογραφήσει το γράμμα 'β'.

Ο πιο διάσημος κρυπτογράφος του 16ου αιώνα ήταν ο Blaise de Vigenere (1523-1596). Το 1585, έγραψε το "Tracte des Chiffres" στο οποίο χρησιμοποίησε έναν πίνακα του Τριθέμιου, αλλά τροποποίησε το μηχανισμό λειτουργίας του κλειδιού. Μία από τις τεχνικές του χρησιμοποιούσε το πρωτότυπο κείμενο ως κλειδί . Μία άλλη χρησιμοποιούσε το κρυπτογραφημένο κείμενο ως κλειδί. Ο τρόπος με τον οποίο αυτά τα κλειδιά χρησιμοποιούνταν είναι γνωστός ως key scheduling, ένα εσωτερικό κεφάλαιο του αλγορίθμου DES (Data Encryption Standard) για τον οποίο θα μιλήσουμε αργότερα.

Το 1628, ένας **Γάλλος** ο Antoine Rossignol βοήθησε τον στρατό της χώρας του να αντεπιτεθεί στους Ουγενότες, με την αποκωδικοποίηση ενός μυστικού μηνύματος. Μετά από αυτή τη νίκη κλήθηκε αρκετές φορές να λύσει κρυπτογραφήματα για την κυβέρνηση της χώρας του. Χρησιμοποίησε δύο λίστες για να λύνει τα κρυπτογραφήματά του. Στην πρώτη λίστα τα στοιχεία του πρωτότυπου ήταν σε αλφαβητική σειρά και τα στοιχεία του κώδικα ήταν τυχαίας επιλογής. Η άλλη λίστα χρησιμοποιείτο για να εφαρμόσει αποκωδικοποίηση, στην οποία τα στοιχεία κώδικα παρατάσσονταν σε αλφαβητική ή αριθμητική σειρά ενώ τα αντίστοιχα στοιχεία του πρωτότυπου κειμένου ήταν ακανόνιστα. Όταν ο Rossignol πέθανε το 1682, ο γιος του και αργότερα ο εγγονός του, συνέχισαν την εργασία του. Συγχρόνως

υπήρχαν αρκετοί κρυπτογράφοι που εργάζονταν για την Γαλλική κυβέρνηση. Όλοι αυτοί αποτέλεσαν τη γνωστή ομάδα "Cabinet Noir" ή "Black Chamber" (τον «σκοτεινό θάλαμο»). Κατά την πρώτη δεκαετία του 1700, οι "Black Chambers" ήταν διάσημοι στην Ευρώπη. Αυτός ο οργανισμός διάβαζε όλη την εισερχόμενη αλληλογραφία από τις ξένες πρεσβείες, αντέγραφαν τα γράμματα, τα ξανασφράγιζαν και τα επέστρεφαν στο ταχυδρομείο το ίδιο πρωί. Το ίδιο γραφείο διαχειριζόταν επίσης όλες τις άλλες πολιτικές και στρατιωτικές υποκλοπές και κάποιες φορές θα έπρεπε να διαβάσουν περίπου 100 γράμματα την ημέρα.

Στις **αποικίες**, δεν υπήρχε κάποιος κεντρικός οργανισμός κρυπτογράφησης. Η αποκωδικοποίηση γινόταν κατά κύριο λόγο από άτομα που επιδείκνυαν ενδιαφέρον, οι οποίοι είχαν και τα μέσα. Το 1775, ένα γράμμα το οποίο βρέθηκε στα χέρια του Dr Benjamin Church θεωρήθηκε ύποπτο ως κωδικοποιημένο μήνυμα από τους Βρεταννούς, όμως οι Αμερικανοί επαναστάτες δεν ήταν σε θέση να το αποκρυπτογραφήσουν. Το πρόβλημά τους λύθηκε από τον Elbridge Gerry (ο οποίος αργότερα έγινε ο 5ος αντιπρόεδρος) και τον Elisha Porter. Το μήνυμα απέδειξε την ενοχή του Church στην απόπειρά του να ενημερώσει τους συντηρητικούς και αργότερα εξορίστηκε. Ο Benedict Arnold χρησιμοποίησε έναν κωδικό στον οποίο ο κάθε ανταποκριτής έχει ένα ακριβές αντίγραφο από το ίδιο βιβλίο κωδικών (codebook). Κάθε λέξη του πρωτότυπου κειμένου αντικαθίσταται από ένα νούμερο, η θέση του οποίου καθορίζεται μέσα στο βιβλίο (για παράδειγμα, 3.5.2, σημαίνει σελίδα 3, γραμμή 5, λέξη 2). Ο ανταποκριτής του Αρλοντ συνελήφθη και κρεμάστηκε, έτσι το βιβλίο με τους κωδικούς είχε σύντομη χρήση. Επίσης οι επαναστάτες χρησιμοποίησαν κρυπτογραφήματα κατά τη διάρκεια του πολέμου. Οι Samuel Woodhull και Robert Townsend προμήθευαν το στρατηγό George Washington με αρκετές πληροφορίες σχετικά με τη δύναμη και τις κινήσεις των Βρετανικών στρατευμάτων μέσα και γύρω από την πόλη της Νέας Υόρκης. Ο κωδικός που χρησιμοποιούσαν αποτελείτο από αριθμούς που υποκαθιστούσαν τυχαία σημεία στην εξωτερική επιφάνεια του κρυπτογραφημένου κειμένου. Κάθε σημείο αντιστοιχεί σε ένα γράμμα. Μία ηλεκτρική τάση επί του σημείου στην εσωτερική επιφάνεια αντιστοιχεί κάθε φορά σε διαφορετικό γράμμα στην εξωτερική επιφάνεια του κρυπτογραφήματος. Ένας απλός **ρότορας** πραγματοποιεί ένα μονοαλφαβητικό υποκατάστατο για το κρυπτογράφημα. Αυτός ο ρότορας είναι τοποθετημένος σε μία συσκευή που δέχεται το πρωτότυπο κείμενο από το πληκτρολόγιο μιας γραφομηχανής και στέλνει τις αντίστοιχες ηλεκτρικές τάσεις στην επιφάνεια του πρωτότυπου κειμένου. Το κρυπτογραφημένο κείμενο παράγεται από τον ρότορα και είτε τυπώνεται είτε εκπέμπεται.

Το επόμενο βήμα διαφοροποιεί πολύ το ρότορα από τα προηγούμενα συστήματα. Μετά από κάθε γράμμα, ο ρότορας στρέφεται έτσι ώστε να έχουμε μετατόπιση του ενσωματωμένου αλφάβητου κατά ένα γράμμα. Έτσι ο ρότορας είναι ένα "πρωτοπόρο κρυπτογράφημα κλειδιού πολυαλφαβητικής αντικατάστασης με ένα ανακατεμένο αλφάβητο και περίοδο 26". Τότε προστίθεται ένας δεύτερος ρότορας ο οποίος μετατοπίζει την θέση του κατά ένα σημείο κάθε φορά που ο πρώτος ρότορας έχει ολοκληρώσει μια πλήρη περιστροφή. Κάθε ηλεκτρικός παλμός οδηγείται μέσα από τους δύο ρότορες έτσι που να κρυπτογραφείται δύο φορές. Από την στιγμή που οι δύο ρότορες κινηθούν, το αλφάβητο τώρα θα έχει μια περίοδο των 676. Όσοι περισσότεροι ρότορες προστίθενται η περίοδος αυξάνει δραματικά: με τρεις ρότορες η περίοδος είναι 17576, με τέσσερις είναι 456976, με πέντε είναι 11881376. Για να σπάσει με συχνοτική ανάλυση, κρυπτογράφημα σε διάταξη με πέντε ρότορες, το κρυπτογραφημένο κείμενο θα είναι εξαιρετικά μεγάλο.

Το σύστημα του ρότορα μπορεί να σπάσει επειδή, αν βρεθεί μια επανάληψη στα πρώτα 26 γράμματα, ο κρυπταναλυτής γνωρίζει ότι μόνο ο πρώτος ρότορας έχει κινηθεί και ότι οι συνδέσεις μεταβάλλονται μόνο από αυτή την κίνηση. Κάθε διαδοχική ομάδα από 26 γράμματα έχει αυτή την ιδιότητα και χρησιμοποιώντας εξισώσεις ο κρυπταναλυτής μπορεί να προσδιορίσει πλήρως αυτόν το ρότορα, απαλοίφοντας έτσι έναν ρότορα από το όλο πρόβλημα. Αυτό μπορεί να επαναληφθεί για κάθε διαδοχικό ρότορα όπως και ο προηγούμενος ρότορας αναγνωρίστηκε, με το πρόσθετο πλεονέκτημα ότι μεγάλωσαν οι περίοδοι πράγμα που οδηγεί σε πολύ μεγάλο αριθμό επαναλήψεων. Αυτό είναι κάπως

πολύπλοκο για να γίνει με το χέρι.

Το 1883, ο Auguste Kerckhoffs έγραψε την "La Cryptographie Militaire" (στρατιωτική κρυπτογραφία), στην οποία όρισε έξι βασικές προδιαγραφές της κρυπτογραφίας.

1. Το κρυπτοκείμενο πρέπει να είναι απαραβίαστο στην πράξη.
2. Το κρυπτοσύστημα πρέπει να είναι κατάλληλο για τους αποδέκτες του.
3. Το κλειδί πρέπει να το θυμόμαστε και να το αντικαθιστούμε εύκολα.
4. Το κρυπτοκείμενο πρέπει να είναι εκπέμψιμο από τηλέγραφο.
5. Ο εξοπλισμός κρυπτογράφησης πρέπει να είναι φορητός.
6. Η μηχανή κρυπτογράφησης πρέπει να είναι σχετικά εύκολη στη χρήση.

Είναι σημαντικό να σημειωθεί ότι τα κλειδιά τα οποία είναι εύκολο να θυμόμαστε είναι πολύ ευάλωτα σε εισβολές και ότι αυτοί οι κανόνες, όπως και όλοι οι άλλοι, πρέπει να εξεταστούν πριν τους αποδεχτούμε.

1.3.3 20^{ος} Αιώνας

Στις αρχές του 20^{ου} αιώνα ο πόλεμος φαινόταν να έρχεται στην Ευρώπη. Η **Αγγλία** αφιέρωσε μια αξιόλογη προσπάθεια στην βελτίωση της κρυπταναλυτικής της δυνατότητας έτσι ώστε με την έναρξη του πολέμου ήταν σε θέση να λύσει τα περισσότερα εχθρικά κρυπτογραφήματα. Η ομάδα των κρυπταναλυτών ονομαζόταν "Room 40" λόγω της αρχικής της θέσης σε ένα συγκεκριμένο κτίριο στο Λονδίνο. Το μεγάλο τους επίτευγμα ήταν η επίλυση κρυπτογραφημάτων του πολεμικού ναυτικού των Γερμανών. Αυτές οι λύσεις ήταν εξαιρετικά απλές γιατί οι Γερμανοί χρησιμοποιούσαν συχνά πολιτικές και εθνικιστικές λέξεις ως κλειδιά, και άλλαζαν τα κλειδιά τους σε τακτικά διαστήματα.

Κατά την διάρκεια της **ποτοαπαγόρευσης στις Η.Π.Α**, το αλκοόλ μεταφερόταν εντός της χώρας από παράνομους λαθρέμπορους, οι οποίοι χρησιμοποίησαν κωδικοποιημένες ραδιοεπικοινωνίες για να ελέγξουν την παράνομη διακίνηση και να αποφύγουν τα περίπολα της ακτοφυλακής. Στην προσπάθεια να κρυφτούν από την ακτοφυλακή, οι λαθρέμποροι χρησιμοποίησαν ένα περίπλοκο σύστημα από κωδικούς και κρυπτογραφήματα. Η ακτοφυλακή προσέλαβε την Elizabeth Smith Friedman για να αποκρυπτογραφήσει αυτούς τους κώδικες και έτσι ανάγκασε τους λαθρέμπορους να χρησιμοποιήσουν πιο περίπλοκους κώδικες και να αλλάζουν πιο συχνά τα κλειδιά τους. Παρόλα αυτά, η αποκρυπτογράφος κατόρθωσε να στείλει αρκετούς λαθρέμπορους στη φυλακή.

Κατά την διάρκεια του **2^{ου} παγκοσμίου πολέμου**, η ουδέτερη χώρα της **Σουηδίας** είχε μία από τις πιο αποτελεσματικές υπηρεσίες κρυπτανάλυσης στον κόσμο. Συγκροτήθηκε το 1936 και την εποχή που ο πόλεμος ξεκινούσε, απασχολούσε 22 άτομα. Η υπηρεσία ήταν κατανεμημένη σε ομάδες και κάθε μία εμπλεκόταν με μια συγκεκριμένη γλώσσα. Οι Σουηδοί ήταν πολύ αποτελεσματικοί στην ερμηνεία των μηνυμάτων από όλα τα εμπόλεμα έθνη. Βοηθήθηκαν ωστόσο και από το γεγονός ότι τα μηνύματα που λάμβαναν ήταν συχνά πρόχειρα ή μερικώς κρυπτογραφημένα.

Επίσης κατά την διάρκεια του 2^{ου} παγκοσμίου πολέμου, οι **Αμερικανοί** είχαν μια σπουδαία επιτυχία στο σπάσιμο Γιαπωνέζικων κωδικών, ενώ οι **Ιάπωνες** αδυνατούσαν να σπάσουν κώδικες των ΗΠΑ. Η κρυπτανάλυση χρησιμοποιήθηκε για να ανατραπεί η Ιαπωνική εισβολή στο Midway, μια καθοριστική μάχη στον Νότιο Ειρηνικό. Οι ΗΠΑ διάβαζαν τακτικά Ιαπωνικούς κώδικες πριν την επίθεση στο Pearl Harbor και γνώριζαν για την κήρυξη του πολέμου που όμως γνωστοποιήθηκε στην κυβέρνηση μόλις μετά την επίθεση στο Pearl Harbor. Οι **Γερμανικοί** κώδικες στον 2^{ο} παγκόσμιο πόλεμο κυριαρχούσαν. Βασίζονταν στην μηχανή "Enigma", η οποία ήταν μια εξέλιξη της μηχανής ρότορα που περιγράψαμε νωρίτερα. Μια Βρετανική ομάδα κρυπτανάλυσης, σε σύμπραξη με μια ομάδα κρυπταναλυτών της αστυνομίας, παραβίασε την "Enigma" πριν τον πόλεμο και κάποιες από τις πρώτες χρήσεις των υπολογιστών ήταν για την αποκωδικοποίηση των κρυπτογραφημάτων "Enigma"

υποκλέπτοντας έτσι από τους Γερμανούς. Το γεγονός αυτό του σπάσιμου αυτών των κωδικών ήταν ύψιστης ευαισθησίας που προώθησε τη γνώση για τις αεροπορικές επιδρομές στην Αγγλία, η οποία ωστόσο δεν αξιοποιήθηκε για κατάσταση ετοιμότητας απέναντι στους βομβαρδισμούς. Αντί αυτού δόθηκε περισσότερη εμπιστοσύνη στα ραντάρ και οι αεροπορικές επιδρομές ανακοινώθηκαν πολύ λίγο πριν τη ρίψη των βομβών.

Το 1948 ο **Shannon** δημοσιοποίησε τη «θεωρία συστημάτων απόρρητων επικοινωνιών». Ο Shannon ήταν ένας από τους πρώτους σύγχρονους κρυπτογράφους που εισήγαγε προηγμένες μαθηματικές τεχνικές στην επιστήμη της κρυπτογραφίας. Αν και η χρήση της συχνοτικής ανάλυσης για επίλυση κρυπτογραφημένων υποκατάστατων ξεκίνησε αρκετά χρόνια νωρίτερα, η ανάλυση του Shannon επέδειξε αρκετά σπουδαία χαρακτηριστικά στην στατιστική φύση της γλώσσας που έκανε την επίλυση σε όλα σχεδόν τα προηγούμενα κρυπτογραφήματα, πολύ εύκολη. Ίσως το πιο σπουδαίο αποτέλεσμα στην περίφημη εργασία του Shannon ήταν η ανάπτυξη μιας μεθόδου μέτρησης της κρυπτογραφικής ισχύος ονομαζόμενη μοναδιαία απόσταση (unicity distance).

Η ιστορία της κρυπτογραφίας θα μπορούσε να τελειώσει αν δεν υπήρχαν πρακτικά προβλήματα, όπως π.χ., για να αποσταλεί ένα μυστικό μήνυμα θα πρέπει πρώτα να σταλεί ένα μυστικό κλειδί. Για τις περισσότερες ανθρώπινες (και υπολογιστικές) γλώσσες, ένα κλειδί δεδομένου μήκους μπορεί να εγγυηθεί ασφάλεια μόνο για 2-3 φορές το μήκος του κλειδιού. Από αυτό προκύπτει ότι κάθε σύστημα με ένα πεπερασμένο κλειδί είναι καταδικασμένο να αποτύχει, αλλά αρκετές εργασίες πρέπει ακόμη να δημοσιευτούν πριν όλη η ελπίδα για την κρυπτογραφία πεπερασμένου κλειδιού εγκαταλειφθεί.

Η ιστορία της κρυπτογραφίας δεν σταματά εδώ. Υπεράριθμες ερευνητικές εργασίες συνεχίζουν να δημοσιεύονται μέχρι σήμερα. Η συμβολή της κρυπτογραφίας στις μοντέρνες δικτυακές εφαρμογές είναι ανεκτίμητη. Μερικές από τις σύγχρονες μεθόδους κρυπτογράφησης επιχειρεί να παρουσιάσει η διπλωματική αυτή εργασία.

1.4 Οργάνωση

Το **Κεφαλαίο 2** περιγράφει βασικές μεθόδους κρυπτογράφησης και παρουσιάζει ενδιαφέρουσα συλλογή αλγορίθμων που τις υλοποιούν. Οι αλγόριθμοι απομυθοποιούνται και ανάγονται σε απλές προσθαφαιρέσεις διακριτών λογαρίθμων.

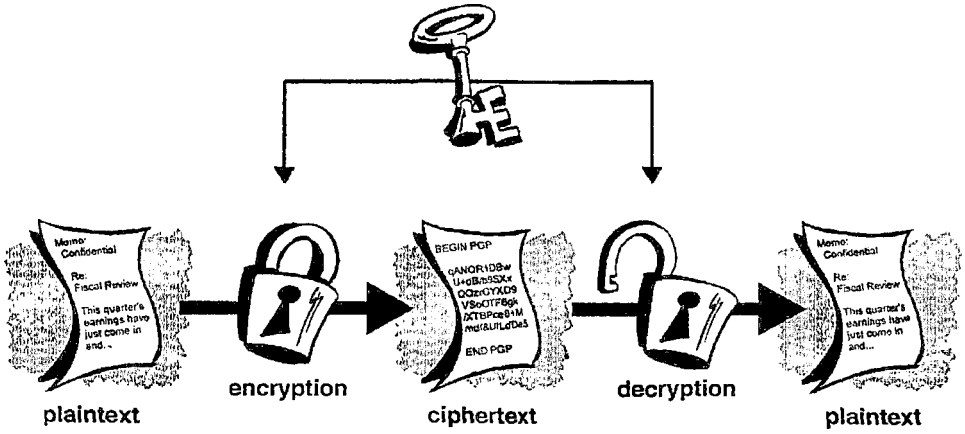
Θέματα ασφάλειας ηλεκτρονικού ταχυδρομείου αναλύονται στο **Κεφάλαιο 3**, στο οποίο επίσης παρουσιάζονται οι σχεδιαστικές αρχές και η βασική δομή του ευρέως διαδεδομένου συστήματος ασφάλειας ηλεκτρονικού ταχυδρομείου PGP (Pretty Good Privacy).

Το **Κεφάλαιο 4** επικεντρώνεται στο περιβάλλον εργασίας του PGP. Γίνεται μια προσέγγιση στο εγχειρίδιο χρήσης της έκδοσης PGP 8.0. Αναλύονται οι βασικές οθόνες του, η δημιουργία των κλειδιών και εφαρμογές του στο ηλεκτρονικό ταχυδρομείο. Είναι ένα μικρό τμήμα από το πολύχρηστο λογισμικό. Το μέγεθος και οι πολλαπλές του χρήσεις φαίνονται συνοπτικά στην υποενότητα επιλογών (Options) του PGP.

2 ΑΛΓΌΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

2.1 Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης

Στη συμμετρική κρυπτογραφία οι αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί τόσο για τη διαδικασία της κρυπτογράφησης όσο και της αποκρυπτογράφησης όπως φαίνεται στο Σχήμα 7.



Σχήμα 7: Μέθοδος Συμμετρικής Κρυπτογράφησης

Οι συμμετρικοί αλγόριθμοι χωρίζονται σε δύο κατηγορίες: στους αλγόριθμους ομάδας (block ciphers) και στους αλγόριθμους στοιχειοσειράς (stream ciphers). Στους αλγορίθμους ομάδας όταν κρυπτογραφείται ένα μήνυμα, ο αλγόριθμος δεν κρυπτογραφεί το κάθε ένα bit του μηνύματος ξεχωριστά αλλά κρυπτογραφεί ολόκληρες ομάδες από bits. Αντίθετα, στους συμμετρικούς αλγόριθμους στοιχειοσειράς ο αλγόριθμος εφαρμόζεται σε μια στοιχειοσειρά από bits. Η ενότητα αυτή θα επικεντρωθεί στην κατηγορία αλγορίθμων ομάδας που περιέχει τους πιο γνωστούς αλγόριθμους κρυπτογράφησης.

Το κρυπτογράφημα ομάδας μετατρέπει μια ομάδα απλού κειμένου (plain text) καθορισμένου μήκους, σε ομάδα κρυπτογραφημένου κειμένου (cipher text) του ιδίου μήκους. Αυτός ο μετασχηματισμός πραγματοποιείται με τη βοήθεια ενός μυστικού κλειδιού. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται μέγεθος ομάδας (block size) και για πολλούς αλγορίθμους κρυπτογράφησης είναι τα 64 bits.

Στα περισσότερα κρυπτογραφήματα ομάδας, η λειτουργία της κρυπτογράφησης ενός τμήματος κειμένου αποτελεί μια διαδικασία που απαιτεί πολλούς κύκλους για την ολοκλήρωσή της. Σε κάθε κύκλο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υποκλειδί. Ο αριθμός των υποκλειδιών συνήθως εξάγεται από το μυστικό κλειδί που προμηθεύει ο χρήστης με τη βοήθεια κάποιας ειδικής συνάρτησης. Το σύνολο των υποκλειδιών ονομάζεται λίστα κλειδιών. Ο αριθμός των κύκλων σε ένα επαναλαμβανόμενο κρυπτογράφημα εξαρτάται τόσο από το επιθυμητό επίπεδο ασφάλειας, όσο και από την επιθυμητή σχέση με την απόδοση. Στις περισσότερες περιπτώσεις, ο μεγαλύτερος αριθμός κύκλων θα αυξήσει την παρεχόμενη ασφάλεια για το κρυπτογράφημα ομάδας, αλλά παράλληλα θα αυξήσει και το χρόνο που απαιτείται για να γίνει η κρυπτογράφηση μειώνοντας την απόδοση.

Μεγάλη συλλογή από συμμετρικούς αλγορίθμους παρουσιάζεται στα βιβλία [Π03, S96, MOV96]. Πιο συγκεκριμένα, οι αλγόριθμοι DES και 3-DES παρουσιάζονται στις αναφορές [Δ11, FIPS77, Π03, S96, MOV96, Δ1, Δ2]. Ο αλγόριθμος CAST-128 περιγράφεται στις [S96, Δ3], ενώ ο IDEA παρουσιάζεται στην [Π03, S96, MOV96, Δ4]. Οι αλγόριθμοι αυτοί

παρουσιάζονται αναλυτικά στη συνέχεια.

2.1.1 Κρυπτογράφημα Ομάδας

Αποτελεί τύπο αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει μια ομάδα μη κρυπτογραφημένου κειμένου (plaintext) καθορισμένου μήκους, σε ομάδα κρυπτογραφημένου κειμένου (ciphertext) του ίδιου μήκους. Αυτός ο μετασχηματισμός γίνεται με τη βοήθεια ενός μυστικού κλειδιού. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται μέγεθος ομάδας (block size) και για πολλούς αλγόριθμους κρυπτογράφησης είναι τα 64-bits. Μελοντικά προβλέπεται αύξηση του μήκους στα 128-bits, καθώς οι υπολογιστές γίνονται ολοένα και πιο ισχυροί. Κάθε κείμενο στο οποίο εφαρμόζεται το κρυπτογράφημα ομάδας δίνει διαφορετικό κρυπτογραφημένο κείμενο.

Όταν χρησιμοποιούμε έναν αλγόριθμο ομάδας για να κρυπτογραφήσουμε ένα μήνυμα αυθαίρετου μήκους, χρησιμοποιούμε τεχνικές που είναι γνωστές ως καταστάσεις λειτουργίας (modes) για το κρυπτογράφημα ομάδας. Για να είναι χρήσιμη μία κατάσταση λειτουργίας πρέπει να είναι τόσο ασφακής και ικανή όσο και ο αλγόριθμος κρυπτογράφησης. Οι καταστάσεις μπορεί να έχουν πρόσθετα χαρακτηριστικά σε σχέση με αυτά που κληρονομούνται από τον αλγόριθμο που χρησιμοποιείται κάθε φορά. Οι τυπικές καταστάσεις του αλγορίθμου DES που αποτελεί χαρακτηριστικό παράδειγμα αυτής της κατηγορίας είναι τέσσερις και έχουν δημοσιευθεί στο FIPS (Federal Information Processing Standards Publications) το 1981 ενώ είναι γνωστές και ως ANSI X3.106. Οι καταστάσεις αυτές είναι οι:

- Electronic Code Book
- Cipher Block Chaining
- Cipher Feedback
- Output Feedback

2.1.1.1 Επαναληπτικές διαδικασίες

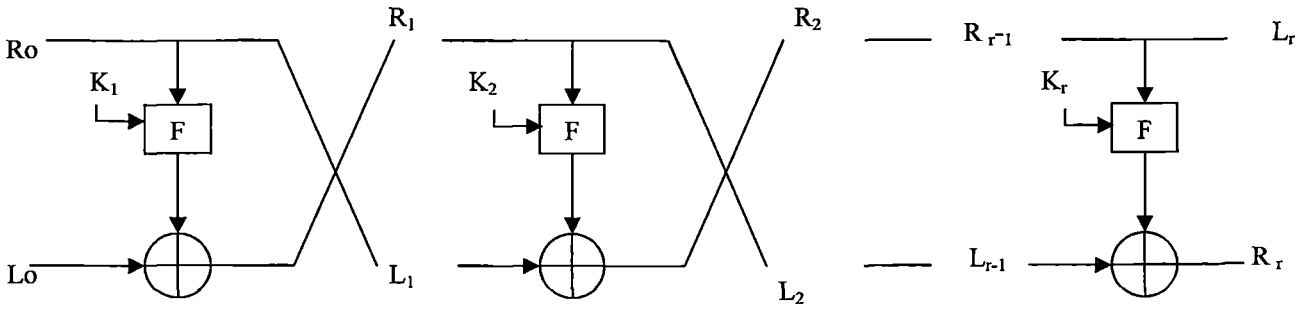
Στα περισσότερα κρυπτογραφήματα ομάδας, η λειτουργία της κρυπτογράφησης ενός τμήματος κειμένου αποτελεί μια διαδικασία που απαιτεί πολλούς κύκλους για την ολοκλήρωσή της. Σε κάθε κύκλο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υποκλειδί. Ο αριθμός των υποκλειδιών συνήθως εξάγεται από το μυστικό κλειδί που προμηθεύει ο χρήστης με τη βοήθεια κάποιας ειδικής συνάρτησης. Το σύνολο των υποκλειδιών ονομάζεται λίστα κλειδιών. Ο αριθμός των κύκλων σε ένα επαναλαμβανόμενο κρυπτογράφημα εξαρτάται τόσο από το επιθυμητό επίπεδο ασφάλειας όσο και από την επιθυμητή σχέση με την απόδοση. Στις περισσότερες περιπτώσεις, ο μεγαλύτερος αριθμός κύκλων θα αυξήσει την παρεχόμενη ασφάλεια για το κρυπτογράφημα ομάδας αλλά παράλληλα θα αυξήσει και τον χρόνο που απαιτείται για να γίνει η κρυπτογράφηση μειώνοντας την απόδοση.

Τα κρυπτογραφήματα Feistel αποτελούν παράδειγμα επαναληπτικών κρυπτογραφημάτων ομάδας, όπου το κρυπτογράφημα υπολογίζεται από το αρχικό κείμενο με επαναληπτική εφαρμογή του ίδιου μετασχηματισμού. Τα κρυπτογραφήματα Feistel τα συναντούμε στη βιβλιογραφία και ως κρυπτογραφήματα τύπου DES.

Στο κρυπτογράφημα Feistel το κείμενο που πρόκειται να κρυπτογραφηθεί χωρίζεται σε δύο ίσα τμήματα. Ο μετασχηματισμός F εφαρμόζεται στο πρώτο μισό χρησιμοποιώντας ένα υποκλειδί ενώ η έξοδος του μετασχηματισμού γίνεται XOR με το υπόλοιπο μισό. Στη συνέχεια, τα δύο μισά αντιμετατίθενται. Κάθε κύκλος ακολουθεί την ίδια διαδικασία εκτός από τον τελευταίο κύκλο όπου και δεν υπάρχει εναλλαγή.

ένα σημαντικό χαρακτηριστικό του κρυπτογραφήματος Feistel είναι ότι τόσο η κρυπτογράφηση όσο και η αποκρυπτογράφηση είναι δομικά πανομοιότυπες αν και τα υποκλειδιά που χρησιμοποιούνται σε κάθε κύκλο για την κρυπτογράφηση χρησιμοποιούνται

επίσης και για τη διαδικασία της αποκρυπτογράφησης με την αντίστροφη όμως σειρά.



Σχήμα 8: Το κρυπτογράφημα Feistel

2.1.2 Ο αλγόριθμος DES

Το Μάιο του 1973 το Εθνικό Γραφείο Προτύπων (National Bureau of Standards, NBS) εξέδωσε μια ανακοίνωση με την οποία ζητούσε προτάσεις για αλγορίθμους κρυπτογράφησης για την προστασία των δεδομένων κατά τη μετάδοση και την αποθήκευσή τους. Στις 6 Αυγούστου του 1974, η IBM ήταν η μόνη που υπέβαλλε υποψηφιότητα με τον αλγόριθμο LUCIFER. Με τη βοήθεια της NSA (National Security Agency), ο αρχικός αλγόριθμος τροποποιήθηκε και στις 15 Ιουλίου του 1977 η τροποποιημένη έκδοση του αλγορίθμου LUCIFER έγινε αποδεκτή από την NBS ως πρότυπο κρυπτογράφησης δεδομένων (Data Encryption Standard - DES).

Ο αλγόριθμος DES έγινε γρήγορα αποδεκτός από την κυβέρνηση των Η.Π.Α και σε άλλες κυβερνήσεις. Έτσι, σήμερα είναι ο πιο διαδεδομένος αλγόριθμος σε όλο τον κόσμο. Για πολλά χρόνια, ο αλγόριθμος DES ήταν σύμφωνος με τη λέξη κρυπτογραφία. Πρόσφατα όμως η αξιοπιστία του δέχτηκε ισχυρότατο χτύπημα από το ίδρυμα Electronic Frontier Foundation το οποίο κατασκεύασε ένα μηχάνημα αξίας 220.000 δολαρίων που μπορούσε να παραβιάζει τα κρυπτογραφημένα με DES μηνύματα. Ωστόσο, υπάρχει η πρόβλεψη πως ο αλγόριθμος θα συνεχίσει να χρησιμοποιείται από τις κυβερνητικές υπηρεσίες και τις τράπεζες για τα επόμενα χρόνια μέσω μιας τροποποιημένης έκδοσης του, που ονομάζεται Triple-DES.

Ο DES είναι συμμετρικός αλγόριθμος ομάδας συνεπώς εφαρμόζεται σε ομάδες του απλού κειμένου με καθορισμένο μέγεθος, 64 bits και δημιουργεί κρυπτογραφημένες ομάδες με το ίδιο μέγεθος. Κατά αυτόν τον τρόπο, ο DES καταλήγει σε αντιμετάθεση μεταξύ 2^{64} πιθανών διευθετήσεων των 64 bits, το κάθε ένα από τα οποία μπορεί να λάβει την τιμή 0 ή 1. Κάθε ομάδα των 64 bits του αρχικού μηνύματος διαχωρίζεται σε δύο ομάδες των 32 bits, L και R (αυτή η διαίρεση χρησιμοποιείται μόνο σε συγκεκριμένες εφαρμογές)

Για την περιγραφή της λειτουργίας του αλγόριθμου DES, κρίνεται σκόπιμο να γίνει αναφορά στις τέσσερις καταστάσεις λειτουργίας του.

2.1.2.1 Electronic Code Book (ECB)

Στη μέθοδο ECB, κάθε ομάδα απλού κειμένου κρυπτογραφείται ανεξάρτητα με το κρυπτογράφημα ομάδας. Κάθε ομάδα των 64-bits της εισόδου κρυπτογραφείται χρησιμοποιώντας το ίδιο κλειδί και το αποτέλεσμα είναι μια καινούρια ομάδα από 64 bits. Η μέθοδος αυτή εκτελεί απλή κρυπτογραφία, χρησιμοποιώντας μια ομάδα κάθε φορά, χωρίς να μπορεί να καθορίσει εάν έχουν εξαχθεί ή αφαιρεθεί τμήματα από το αρχικό μήνυμα. Έχει αρκετά καλή απόδοση, όταν χρησιμοποιείται σε κανάλια μεταδόσεων με θόρυβο, αφού η αλλαγή μερικών bits επηρεάζει μόνο μια ομάδα των 64 bits.

Η μέθοδος ECB είναι τόσο ασφαλής όσο είναι το κρυπτογράφημα ομάδας που χρησιμοποιείται. Κάθε ομάδα απλού κειμένου δίνει μια πανομοιότυπη ομάδα κρυπτογραφημένου κειμένου. Η ταχύτητα για κάθε κρυπτογράφηση είναι ίδια με αυτή του

κρυπτογραφήματος ομάδας. Η μέθοδος ECB μπορεί εύκολα να παραλληλιστεί ώστε να αυξηθεί η ταχύτητά της.

2.1.2.2 Cipher Block Chaining (CBC)

Στη μέθοδο CBC, σε κάθε ομάδα κειμένου εφαρμόζεται η συνάρτηση XOR με δεύτερο μέλος την κρυπτογραφημένη τιμή της προηγούμενης ομάδας και στη συνέχεια η έξοδος αυτού κρυπτογραφείται χρησιμοποιώντας το κλειδί. Αρχικά, για τη διαδικασία χρησιμοποιείται ένα διάνυσμα αρχικοποίησης C_0.

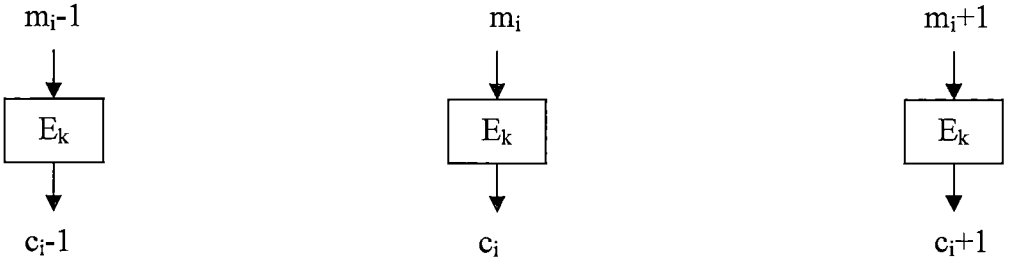
Σε αυτόν τον τρόπο λειτουργίας, αντίθετα με τον προηγούμενο, στο αποτέλεσμα αποκρύπτονται επαναλαμβανόμενοι χαρακτήρες του αρχικού κειμένου.

Η μέθοδος CBC είναι τόσο ασφαλής όσο είναι και το κρυπτογράφημα ομάδας που χρησιμοποιείται. Το απλό κείμενο δεν μπορεί να παραποιηθεί παρά μόνο αν αφαιρεθούν τμήματα από την αρχή ή το τέλος του κρυπτογραφήματος. Επιπλέον, το διάνυσμα αρχικοποίησης C_0 πρέπει να είναι διαφορετικό για κάθε δύο μηνύματα κρυπτογραφημένα με το ίδιο κλειδί και προτείνεται να επιλέγεται με τυχαίο τρόπο. Το κλειδί δεν είναι απαραίτητο να είναι κρυπτογραφημένο και μπορεί να μεταδίδεται μαζί με το κρυπτογραφημένο κείμενο. Η ταχύτητα κρυπτογράφησης είναι ίση με αυτή του κρυπτογραφήματος ομάδας, ωστόσο δε μπορεί εύκολα να παραλληλιστεί.

2.1.2.3 Cipher Feedback (CFB)

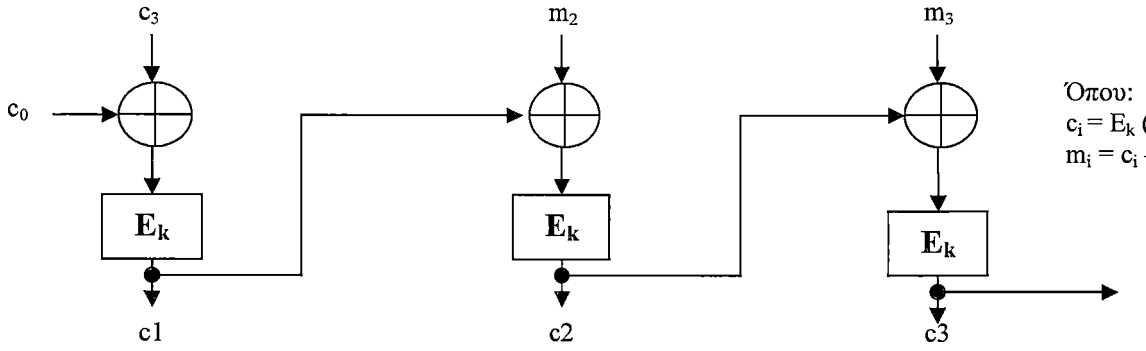
Στη μέθοδο CFB, η προηγούμενη κρυπτογραφημένη ομάδα κρυπτογραφείται (με την τιμή του κλειδιού του χρήστη χρησιμοποιώντας τον τρόπο λειτουργίας EBC) και η έξοδος που παράγεται συνδυάζεται με το τμήμα του απλού κειμένου χρησιμοποιώντας την συνάρτηση XOR ώστε να παράγουν την τρέχουσα κρυπτογραφημένη ομάδα. Αυτός ο τρόπος λειτουργίας είναι αυτοσυγχρονιζόμενος και επιτρέπει στον χρήστη να αποκρυπτογραφήσει μόνο ένα μέρος κάποιου μηνύματος, αρχίζοντας από μια σταθερή απόσταση πριν από την αρχή των επιθυμητών δεδομένων. Είναι δυνατό να οριστεί η μέθοδος CFB με τέτοιο τρόπο ώστε να χρησιμοποιεί πληροφορία η οποία να είναι μικρότερη από μια ολόκληρη ομάδα δεδομένων.

Η μέθοδος CFB είναι τόσο ασφαλής όσο είναι το κρυπτογράφημα στο οποίο εφαρμόζεται. Το απλό κείμενο δε μπορεί να παραποιηθεί παρά μόνο αν αφαιρεθούν τμήματα από την αρχή ή το τέλος του κρυπτογραφήματος. Στη μέθοδο CFB εάν χρησιμοποιηθεί ολόκληρη η πληροφορία της ομάδας ως είσοδος του επόμενου σταδίου, τότε, στην περίπτωση που δύο κρυπτογραφημένες ομάδες είναι όμοιες, οι αντίστοιχες έξοδοι του επόμενου βήματος θα είναι επίσης όμοιες. Ο παραπάνω μηχανισμός επιτρέπει τη διαρροή πληροφορίας που σχετίζεται με το απλό κείμενο. Όταν χρησιμοποιείται ολόκληρη η πληροφορία της ομάδας για τα επόμενα στάδια, τότε η ταχύτητα της κρυπτογράφησης ταυτίζεται με αυτή του αλγόριθμου και η όλη διαδικασία μπορεί εύκολα να παραλληλιστεί.



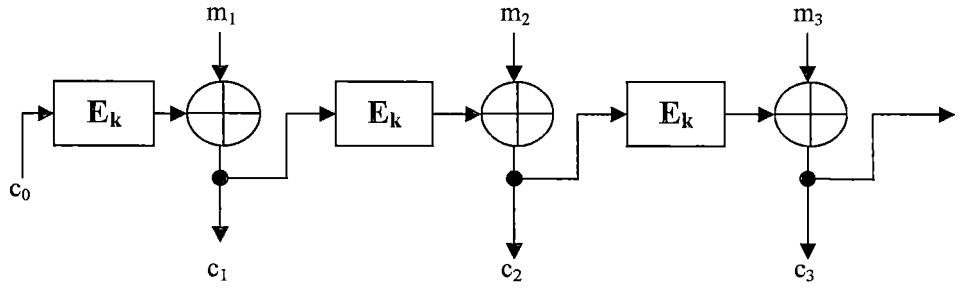
Όπου:
$c_i = E_k (m_i)$
$m_i = D_k (c_i)$

(α) Η μέθοδος Electronic Code Book



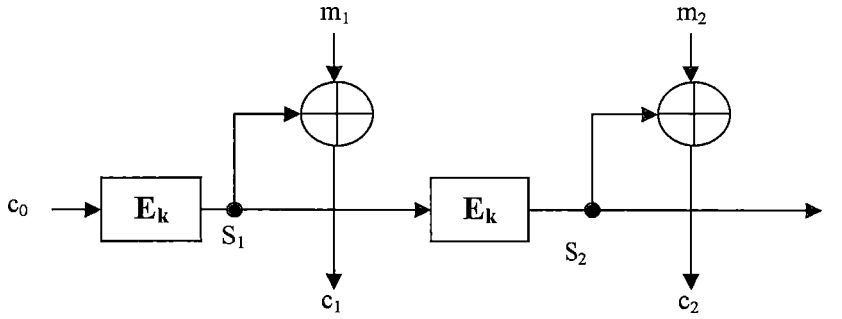
Όπου:
$c_i = E_k (c_i\text{-}1 \oplus m_i)$
$m_i = c_i - 1 \oplus D_k (c_i)$

(β) Η μέθοδος Cipher Block Chaining



Όπου:
$c_i = E_k (c_i\text{-}1 \oplus m_i)$
$m_i = E_k (c_i - 1) \oplus c_i$

(γ) Η μέθοδος Cipher Feedback



Όπου:
$c_i = m_i \quad S_i$
$m_i = c_i \quad S_i$
$S_i = E_k (S_i - 1)$

(δ) Η μέθοδος Output Feedback

Σχήμα 9: Οι Καταστάσεις λειτουργίας του αλγόριθμου DES.

2.1.2.4 Output Feedback (OFB)

Η μέθοδος OFB είναι παρόμοια με τη CFB με τη μόνη διαφορά ότι η ποσότητα πληροφορίας στην οποία εφαρμόζεται η συνάρτηση XOR με την ομάδα απλού κειμένου δημιουργείται ανεξάρτητα από το απλό κείμενο ή το κρυπτογράφημα.

Και σε αυτή την περίπτωση, το αποτέλεσμα που προκύπτει επανατροφοδοτείται στην είσοδο του μηχανισμού κρυπτογράφησης. Ένας καταχωρητής αρχικοποιείται με μια γνωστή τιμή και στη συνέχεια κρυπτογραφείται με το κλειδί του χρήστη, χρησιμοποιώντας τον τρόπο ECB. Το αποτέλεσμα της διαδικασίας αυτής χρησιμοποιείται ως το κλειδί για την κρυπτογράφηση της ομάδας δεδομένων και αποθηκεύεται ξανά στον καταχωρητή για να χρησιμοποιηθεί στην επόμενη ομάδα. Αυτός ο τρόπος λειτουργίας παράγει μια ακολουθία bits κλειδιού που μπορεί να χρησιμοποιηθεί για μικρά λάθη κατά τη μεταφορά, με καλή απόδοση για την κρυπτογράφηση και αποκρυπτογράφηση επικοινωνιών.

Πιο αναλυτικά, ένα διάνυσμα s_0 χρησιμοποιείται ως μήτρα μιας ακολουθίας δεδομένων ομάδας s_0, ενώ κάθε ομάδα δεδομένων s_j εξάγεται από την κρυπτογράφηση της προηγούμενης ομάδας δεδομένων s_{j-1}. Η κρυπτογράφηση της ομάδας απλού κειμένου γίνεται χρησιμοποιώντας τη συνάρτηση XOR ανάμεσα στο τμήμα του αρχικού κειμένου και το σχετιζόμενο τμήμα δεδομένων. Η μέθοδος OFB σε σχέση με τη CFB παρουσιάζει το πλεονέκτημα ότι, αν κατά τη μετάδοση παρουσιαστεί σφάλμα σε ορισμένα bits, τότε αυτά δεν διαδίδονται επηρεάζοντας την αποκρυπτογράφηση των επόμενων ομάδων δεδομένων. Το πρόβλημα με τη μέθοδο OFB είναι ότι το απλό κείμενο μπορεί εύκολα να παραποιηθεί. Για παράδειγμα, ένας επιτιθέμενος που γνωρίζει μια ομάδα απλού κειμένου m_i μπορεί εύκολα να την αντικαταστήσει με μια άλλη ομάδα απλού κειμένου έστω x, με το να εφαρμόσει τη συνάρτηση $XOR(m_i \oplus x)$ στην αντίστοιχη ομάδα κρυπτογράφησης c_i. Υπάρχουν αντίστοιχες επιθέσεις που μπορούν να γίνουν και στις μεθόδους CBC και CFB, αλλά σε αυτές κάποιο τμήμα του απλού κειμένου θα τροποποιηθεί έτσι που να μη μπορεί να μπορεί να προβλεφθεί από τον επιτιθέμενο. Ωστόσο, το πρώτο κρυπτογράφημα ομάδας (το διάνυσμα αρχικοποίησης) στη μέθοδο CBC και το τελευταίο στην CFB μπορούν να παραποιηθούν το ίδιο εύκολα όπως στη μέθοδο OFB. Επιθέσεις τέτοιας μορφής μπορούν να αποφευχθούν με τη χρησιμοποίηση σχημάτων ψηφιακών υπογραφών MAC(Message Authentication Code).

Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του αλγόριθμου κρυπτογράφησης. Αν και η διαδικασία της κρυπτογράφησης δε μπορεί εύκολα να παραλληλιστεί, ωστόσο μπορεί να εξοικονομηθεί χρόνος με τη δημιουργία της στοιχειοσειράς του κλειδιού πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.

Εξαιτίας κάποιων αδυναμιών της μεθόδου OFB, ο Diffie πρότεινε μια άλλη μέθοδο η οποία διαφέρει από την OFB στον τρόπο με τον οποίο οι διαδοχικές ομάδες δεδομένων παράγονται από διαδοχικές κρυπτογραφήσεις. Αντί να εξάγεται μια ομάδα δεδομένων από την κρυπτογράφηση της προηγούμενης ομάδας, ο Diffie πρότεινε να κρυπτογραφείται η ποσότητα $i+Ivmod2^{64}$ για την i ομάδα δεδομένων, όπου το IV αποτελεί κάποιο διάνυσμα αρχικοποίησης.

2.1.3 Ο αλγόριθμος Triple-DES

Ο κίνδυνος της παραβίασης των κρυπτογραφημένων με τον αλγόριθμο DES μηνυμάτων μπορεί να ελαχιστοποιηθεί, χρησιμοποιώντας μια τροποποιημένη έκδοση του DES που ονομάζεται triple-DES. Σύμφωνα με αυτή το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγορίθμου. Αυτό μπορεί να επιτευχθεί με πολλούς τρόπους. Το πρότυπο ANSI X9.52 ορίζει την κρυπτογράφηση με τον triple-DES με κλειδιά k_1, k_2, k_3 ως:

$$C = E_{K3}(D_{K2}(E_{K1}(M)))$$

όπου τα E_k και D_k δηλώνουν DES κρυπτογραφήσεις και αποκρυπτογραφήσεις με το κλειδί k. Αυτή η μέθοδος κρυπτογράφησης συχνά αναφέρεται ως DES-EDE. Όσον αφορά τα κλειδιά, το πρότυπο ANSI X9.52 ορίζει τρεις διαφορετικές περιπτώσεις:

- Τα κλειδιά k_1, k_2, k_3 είναι ανεξάρτητα.
- Τα κλειδιά k_1 και k_2 είναι ανεξάρτητα, αλλά $k_1 = k_3$.
- $k_1 = k_2 = k_3$.

Γενικότερα, υπάρχουν τέσσερις παραλλαγές για τον triple-DES:

- **DES-EEE3 (Encrypt-Encrypt-Encrypt)**: πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις
- **DES-EDE3 (Encrypt-Decrypt-Encrypt)**: το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- **DES-EEE2**: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- **DES-EDE2**: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

Θα εξετάσουμε αναλυτικότερα την τελευταία μέθοδο που είναι η DES-EDE2. Ο αλγόριθμος χρησιμοποιεί δύο κλειδιά των 56 bits. Το πρώτο κλειδί χρησιμοποιείται για να κρυπτογραφούνται τα μηνύματα, με την ίδια διαδικασία που γίνεται και στον DES. Το δεύτερο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση του κατά DES κρυπτογραφημένου μηνύματος. Αφού αυτό το δεύτερο κλειδί δεν είναι κατάλληλο για την αποκρυπτογράφηση, η αποκρυπτογράφηση δεν επαναφέρει το κρυπτογραφημένο μήνυμα στην αρχική του μορφή αλλά ουσιαστικά το κρυπτογραφεί ακόμα περισσότερο. Έπειτα, το διπλά κρυπτογραφημένο μήνυμα κρυπτογραφείται ξανά με το πρώτο κλειδί για να σχηματιστεί το τελικό κρυπτογράφημα. Σε όλες τις περιπτώσεις, το μέγεθος του κλειδιού πρέπει να είναι περίπου 2^{112}.

Αξίζει να αναφερθεί ότι, για τον αλγόριθμο triple-DES, ένας από τους ειδικούς της κρυπτογραφίας, ο Bruce Schneier, δήλωσε ότι "δεν υπάρχει αρκετό πυρίτιο σε ολόκληρο τον γαλαξία ή αρκετός χρόνος μέχρι την κατάρευση του ήλιου για να παραβιαστεί ο triple-DES με την τεχνική της βίαιης επίθεσης (brute force)".

2.1.4 Ο αλγόριθμος CAST-128

Ο CAST-128 ανήκει στους αλγόριθμους κρυπτογράφησης που είναι γνωστοί ως κρυπτογραφήματα Feistel. Η λειτουργία του είναι παρόμοια με αυτή του DES. Ο αλγόριθμος περιγράφεται στα ακόλουθα τέσσερα βήματα:

ΕΙΣΟΔΟΣ: απλό κείμενο m1 ... m64 & κλειδί K = k1... k128

ΕΞΟΔΟΣ: κρυπτοκείμενο c1 ... c64.

1. Υπολογισμός 16 ζευγών από υποκλειδιά {Kmi, Kri} του K.
2. Διαχωρισμός του απλού κειμένου σε αριστερό και δεξιό τμήμα, L0 = m1 ... m32 και R0 = m33 ... m64 (<L0, R0> ← <m1 ... m64>).

3. Υπολογισμός των Li και Ri, επαναληπτικά για 16 βήματα, ως ακολούθως:

   Li = Ri - 1;

   Ri = Li – 1 ^ f(Ri-1, Kmi, Kri) (η συνάρτηση f περιγράφεται στη συνέχεια).

4. Ανταλλαγή των τελικών μπλοκ L16 και R16 και συνένωση για την παραγωγή του κρυπτοκειμένου (c1 ... c64 ← <R16, L16>).

Ο CAST-128 χρησιμοποιεί τρεις διαφορετικούς τύπους συναρτήσεων. Σημειώνουμε ότι παρακάτω τα σύμβολα '+' και '-' παριστάνουν πρόσθεση και αφαίρεση αντίστοιχα υπόλοιπο 2**32, '^' παριστάνει την ανά bit αποκλειστικό-ή (XOR) πράξη και το '<<<' παριστάνει τη λειτουργία της κυκλικής μετατόπισης προς τα αριστερά.

Τύπος 1: I = ((Kmi + D) <<< Kri),

f = ((S1[Ia] ^ S2[Ib]) – S3[Ic]) + S4[Id],

Τύπος 2: I = ((Kmi ^ D) <<< Kri),

f = ((S1[Ia] - S2[Ib]) + S3[Ic]) ^ S4[Id],

Τύπος 3: I = ((Kmi - D) <<< Kri),

f = ((S1[Ia] + S2[Ib]) ^ S3[Ic]) - S4[Id],

όπου D είναι τα δεδομένα εισόδου στην συνάρτηση f, ενώ τα Ia ... Id είναι τα bytes του I, ξεκινώντας από το πιο σημαντικό προς το λιγότερο σημαντικό.

Διαφορετικές επαναλήψεις του κρυπτογραφήματος Feistel χρησιμοποιούν διαφορετικούς τύπους συναρτήσεων.

2.1.5 Ο αλγόριθμος IDEA (International Data Encryption Algorithm)

Η διαδικασία κρυπτογράφησης μηνυμάτων με τον αλγόριθμο IDEA περιλαμβάνει οκτώ βήματα:

Ο IDEA χρησιμοποιεί 52 υποκλειδιά $K_{(1)}$, ... $K_{(52)}$ μήκους 16 bits το καθένα. Δύο υποκλειδιά χρησιμοποιούνται κατάλληλα σε κάθε στάδιο, τέσσερα υποκλειδιά χρησιμοποιούνται πριν από κάθε στάδιο και μετά από το τελευταίο στάδιο. Το τμήμα του μη κρυπτογραφημένου μηνύματος μήκους 64 bits χωρίζεται σε τέσσερα ίσα τμήματα A, B, C, D με μήκος 16 bits το καθένα. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού καθώς και η πράξη XOR χρησιμοποιούνται από τον IDEA για να συνδυαστούν δύο 16 bit τιμές και να σχηματίσουν ένα 16 bit αποτέλεσμα.

Οι πράξεις που εκτελούνται από τον IDEA πριν το πρώτο βήμα είναι οι ακόλουθες:

$$A_0 = AK_{(1)}$$

$$B_0 = B + K_{(2)}$$

$$C_0 = C + K_{(3)}$$

$$D_0 = DK_{(4)}$$

Ακολουθούν οι υπολογισμοί του 1ου βήματος:

$$E = A_0 \oplus C_0$$

$$F = B_0 \oplus D_0$$

$$E' = EK_{(5)}$$

$$F' = E' + F$$

$$F'' = F'K_{(6)}$$

$$E'' = F'' + E'$$

$$A_1 = A_0 \oplus F''$$

$$C_1 = C_0 \oplus F''$$

$$B_1 = B_0 \oplus E''$$

$$D_1 = D_0 \oplus E''$$

$$Swap(B_1, C_1)$$

Για το δεύτερο βήμα η ίδια ακολουθία πράξεων επαναλαμβάνεται ανταλλάσοντας τα υποκλειδιά $K_{(1)}$–$K_{(6)}$ με τα $K_{(7)}$-$K_{(12)}$ και τα τμήματα μηνύματος A, B, C, D με τα τροποποιημένα τμήματα A_1, B_1, C_1 και D_1, αντίστοιχα. Η διαδικασία αυτή επαναλαμβάνεται άλλες έξι φορές για τα επόμενα βήματα αλλά στο τελευταίο (όγδοο) βήμα δεν γίνεται η πράξη swap στα τροποποιημένα τμήματα B8 και C8.

Τέλος, τα κωδικοποιημένα τμήματα του αρχικού μηνύματος προκύπτουν από τις πράξεις:

$$encrypt(A) = A_8K_{(49)}$$

$$encrypt(B) = B_8 + K_{(50)}$$

$$encrypt(C) = C_8 + K_{(51)}$$

$$encrypt(D) = D_8K_{(52)}$$

Συνεχίζουμε με την περιγραφή της διαδικασίας αποκρυπτογράφησης στην οποία τα οκτώ βήματα της διαδικασίας κρυπτογράφησης αναστρέφονται. Η διαδικασία αυτή χρησιμοποιεί διαφορετικά υποκλειδιά από εκείνα της κρυπτογράφησης. Τα κλειδιά αυτά υπολογίζονται ως εξής, j = 0,...,7:

$$DK_{(1)} = 1/K_{(49)}$$

$$DK_{(2)} = -K_{(50)}$$

$$DK_{(3)} = -K_{(51)}$$

$$DK_{(4)} = 1/K_{(52)}$$

$$DK_{(5+6j)} = K_{(47-6j)}$$

$$DK_{(6+6j)} = K_{(48-6j)}$$

$$DK_{(7+6j)} = 1/K_{(43-6j)}$$

$$DK_{(8+6j)} = -K_{(45-6j)}$$

$$DK_{(9+6j)} = -K_{(44-6j)}$$

$$DK_{(10+6j)} = 1/K_{(46-6j)}$$

Τα υποκλειδιά κρυπτογράφησης προκύπτουν από ένα αρχικό κλειδί μήκους 128 bits. Το κλειδί αυτό διαιρείται σε 8 ίσα τμήματα. Τα επόμενα 8 υποκλειδιά $K_{(9)}$ ... $K_{(16)}$ προκύπτουν από το αρχικό κλειδί των 128 bits αφού υποστεί αριστερή κυκλική μετατόπιση (left rotation) κατά 25 bits και χωριστεί και πάλι σε 8 ίσα μέρη. Προκειμένου να παραχθούν τα υπόλοιπα κλειδιά η διαδικασία αυτή επαναλαμβάνεται.

Αξίζει να αναφερθεί ότι ο αλγόριθμος IDEA θεωρείται εξαιρετικά ασφαλής και έχει αντισταθεί σε όλες τις επιθέσεις που έχει δεχθεί μέχρι σήμερα.

2.2 Ασύμμετροι Αλγόριθμοι Κρυπτογράφησης

Τα συστήματα ασύμμετρης κρυπτογράφησης έχουν την ιδιότητα ότι χρησιμοποιούνται ξεχωριστά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση και ότι, αν δοθεί ένα καλά επιλεγμένο κλειδί κρυπτογράφησης, είναι πρακτικά αδύνατο να ανακαλυφθεί το αντίστοιχο κλειδί αποκρυπτογράφησης. Κάτω από αυτές τις ιδιότητες το κλειδί κρυπτογράφησης μπορεί να δημοσιευθεί και να διατηρείται μυστικό μόνο το κλειδί αποκρυπτογράφησης.

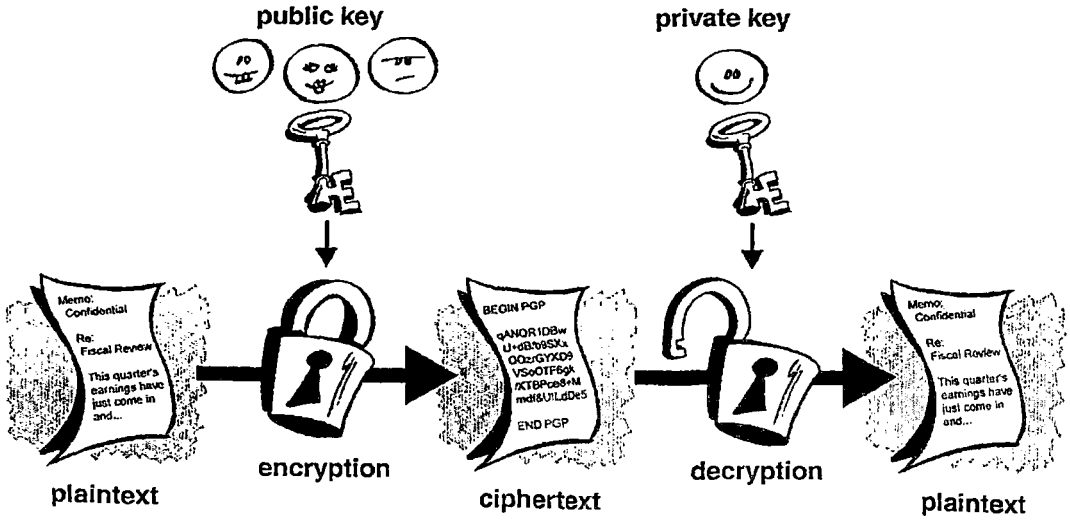
Για να αποκτήσουμε μια αίσθηση της κρυπτογραφίας δημοσίου κλειδιού, ας θεωρήσουμε τις εξής δύο ερωτήσεις:

Ερώτηση 1: Πόσο κάνει 314159265358979 x 314159265358979;

Ερώτηση 2: Ποια είναι η τετραγωνική ρίζα του 3912571506419387090594828508241;

Οι περισσότεροι απόφοιτοι δημοτικού, με ένα μολύβι και χαρτί, μπορούν να απαντήσουν στην Ερώτηση 1 σε μία με δύο ώρες. Αντίθετα, οι περισσότεροι ενήλικες με ένα μολύβι και χαρτί, δεν μπορούν να βρουν τη σωστή λύση στην Ερώτηση 2 χωρίς να χρησιμοποιήσουν αριθμομηχανή, υπολογιστή, ή κάποια άλλη εξωτερική βοήθεια. Παρά το ότι το τετράγωνο και η ρίζα ενός αριθμού είναι αντίστροφες πράξεις, διαφέρουν πολύ στην υπολογιστική τους πολυπλοκότητα. Αυτό το είδος ασυμμετρίας θέτει τις βάσεις της κρυπτογραφίας δημοσίου κλειδιού. Η κρυπτογράφηση χρησιμοποιεί την εύκολη πράξη αλλά η αποκρυπτογράφηση χωρίς το κλειδί απαιτεί την εκτέλεση της δύσκολης πράξης.

Ο τρόπος λειτουργίας της κρυπτογράφησης δημοσίου κλειδιού είναι ο ακόλουθος. Ο χρήστης διαλέγει ένα ζεύγος (δημόσιο κλειδί, ιδιωτικό κλειδί) και δημοσιεύει το δημόσιο κλειδί. Το δημόσιο κλειδί είναι το κλειδί κρυπτογράφησης, ενώ το ιδιωτικό κλειδί είναι το κλειδί αποκρυπτογράφησης. Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη, και του στέλνει το μυστικό μήνυμα. Εφόσον μόνο ο παραλήπτης διαθέτει το ιδιωτικό κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα. Η διαδικασία αυτή παρουσιάζεται στο Σχήμα 10.



Σχήμα 10: Μέθοδος ασύμμετρης κρυπτογράφησης.

Πολλοί ασύμμετροι αλγόριθμοι κρυπτογράφησης παρουσιάζονται στα βιβλία [Π03, S96]. Πιο συγκεκριμένα, ο αλγόριθμος RSA περιγράφεται στις αναφορές [Π03, MOV96, Δ5, Δ6], ενώ ο αλγόριθμος Diffie-Helman παρουσιάζεται στις [Δ7, C01, S96]. Οι αλγόριθμοι αυτοί παρουσιάζονται αναλυτικά στη συνέχεια.

2.2.1 Ο αλγόριθμος RSA

Για την παραγωγή των κρυπτογραφικών κλειδιών του αλγορίθμου RSA αρχικά επιλέγονται δύο πρώτοι αριθμοί P και Q. Οι αριθμοί αυτοί πρέπει να είναι μεγάλοι (π.χ. 1024 bits) και πρέπει να κρατούνται μυστικοί. Έπειτα, επιλέγεται ένας αριθμός E, ώστε ο E να είναι μικρότερος από τον αριθμό N = PQ. Ο αριθμός E δεν είναι απαραίτητο να είναι πρώτος αριθμός, αλλά πρέπει οπωσδήποτε να είναι περιττός. Επιπλέον, οι αριθμοί E και (P-1)(Q-1) πρέπει να είναι συγκριτικά πρώτοι , δηλαδή οι δύο αυτοί αριθμοί δεν πρέπει να έχουν κοινούς πρώτους παράγοντες. Στη συνέχεια, υπολογίζεται ο αριθμός D, έτσι ώστε ο αριθμός DE-1 να διαιρείται τέλεια από τον αριθμό (P-1)(Q-1). Η μαθηματική διατύπωση της πρότασης αυτής έχει ως εξής:

$$(DE) \bmod ((P-1)(Q-1)) = 1,$$

όπου ο αριθμός D ονομάζεται πολλαπλασιαστική ανάστροφος (multiplicative inverse) του αριθμού E. Το ζεύγος των αριθμών (E,PQ) αποτελεί το δημόσιο κλειδί του αλγορίθμου RSA ενώ το ιδιωτικό κλειδί του αλγορίθμου είναι το ζεύγος (D, PQ). Γενικά, είναι δύσκολο για κάποιον σήμερα να μπορέσει να παράγει το ιδιωτικό κλειδί από το δημόσιο. Ωστόσο, αν κάποιος κατάφερνε να παραγοντοποιήσει το N σε P και Q, τότε θα μπορούσε εύκολα να εξάγει και το ιδιωτικό κλειδί D. Γίνεται λοιπόν εύκολα κατανοητό ότι η ασφάλεια του RSA βασίζεται στην παραδοχή ότι η παραγοντοποίηση είναι μια δύσκολη διαδικασία. Ο αλγόριθμος RSA μπορεί να χρησιμοποιηθεί τόσο για κρυπτογράφηση όσο και για τις ψηφιακές υπογραφές.

Η διαδικασία κρυπτογράφησης ενός μηνύματος T με τον αλγόριθμο RSA περιγράφεται στη συνέχεια. Έστω ότι ο χρήστης A θέλει να στείλει ένα μήνυμα T στο χρήστη B.

1. Αρχικά ο RSA παριστάνει το T με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής [0, N-1]. Αν το μήνυμα T είναι πολύ μεγάλο τότε χωρίζεται σε έναν αριθμό μικρότερων κομματιών. Ομοίως, το κάθε κομμάτι παριστάνεται με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής [0, N-1]. Οι αριθμοί που αποδίδονται σε διαφορετικά τμήματα είναι διαφορετικοί, αλλά έχουν το ίδιο σταθερό μήκος.
2. Το κάθε τμήμα του μηνύματος κρυπτογραφείται με βάση τη συνάρτηση κρυπτογράφησης η οποία δίνεται από τη σχέση:

   $$C = \text{encrypt}(T) = T^E \bmod (PQ).$$

   Ο υπολογισμός αυτός μπορεί να γίνει αρκετά γρήγορα με ειδικό λογισμικό που χρησιμοποιεί κατάλληλους αλγορίθμους. Στη συνέχεια, οι αριθμοί που προκύπτουν από την κατάτμηση του αρχικού μηνύματος ενώνονται και σχηματίζουν το κρυπτογραφημένο μήνυμα C.

Η συνάρτηση αποκρυπτογράφησης δίνεται από την ακόλουθη σχέση:

$$\text{decrypt}(C) = C^D \bmod (PQ)$$

Αν το μήνυμα είναι μικρό αποκρυπτογραφείται απευθείας με χρήση της συνάρτησης αποκρυπτογράφησης. Αν το μήνυμα είναι μεγάλο τότε χωρίζεται σε κομμάτια και το κάθε κομμάτι αποκρυπτογραφείται με χρήση της συνάρτησης αποκρυπτογράφησης.

Ο χρήστης B που είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί D μπορεί επομένως να αποκρυπτογραφήσει το μήνυμα.

Παρόμοια διαδικασία ακολουθείται και στις ψηφιακές υπογραφές. Στην περίπτωση αυτή ο παραλήπτης B πρέπει να βεβαιωθεί ότι το μήνυμα είναι αυθεντικό, δεν έχει αλλοιωθεί και είναι από τον A. Η ψηφιακή υπογραφή S που δημιουργεί ο A έχει τη μορφή $S = T^D \bmod (PQ)$, όπου (D,PQ) είναι το ιδιωτικό κλειδί του A. Ο A στέλνει τα T και S στον B. Για να πιστοποιήσει την υπογραφή ο B εξετάζει το $T = S^E \bmod (PQ)$, όπου (E,PQ) είναι το δημόσιο κλειδί του A.

Είναι σημαντικό να τονιστεί ότι η παραπάνω διαδικασίες είναι ασύμμετρες, αφού μόνο το άτομο που γνωρίζει το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα, ενώ η αποκρυπτογράφηση και η πιστοποίηση γίνεται με το δημόσιο κλειδί του αποστολέα.

2.2.2 Ο αλγόριθμος Diffie-Hellman

Η πρώτη δημοσιοποίηση αλγόριθμου δημοσίου κλειδιού εμφανίζεται στην εργασία των Diffie και Hellman. Ένα πλήθος από εμπορικές εφαρμογές αναπτύσσουν αυτή την τεχνική ανταλλαγής κλειδιού.

Ο σκοπός του αλγόριθμου αυτού είναι η παροχή ασφάλειας στην ανταλλαγή ενός κλειδιού ανάμεσα σε δύο χρήστες, το οποίο μπορεί να χρησιμοποιηθεί στη συνέχεια για κρυπτογράφηση μηνυμάτων.

Η αποδοτικότητα του αλγορίθμου Diffie-Hellman βασίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων. Εν συντομία, ο διακριτός λογάριθμος ορίζεται ως ακολούθως. Ορίζουμε πρώτα μια πρωτογενή ρίζα ενός πρώτου αριθμού p να είναι ένας αριθμός του οποίου όλες οι δυνάμεις παράγουν όλους τους ακέραιους από 1 ως p-1. Πιο συγκεκριμένα, αν a είναι μια πρωτογενής ρίζα ενός πρώτου αριθμού p, τότε οι αριθμοί

$$a \bmod p,\ a^2 \bmod p,\ \ldots,\ a^{p-1} \bmod p$$

είναι όλοι διαφορετικοί και η ακολουθία τους αποτελεί μια μετάθεση των αριθμών 1, ..., p-1.

Για κάθε ακέραιο b και για κάθε πρωτογενή ρίζα a ενός πρώτου αριθμού p, είναι δυνατή η εύρεση ενός μοναδικού εκθέτη i τέτοιου ώστε

$$b = a^i \bmod p, \text{ όπου } 0 \le i \le (p-1).$$

Ο εκθέτης i αναφέρεται ως διακριτός λογάριθμος (ή δείκτης) του b, με βάση a, mod p και συμβολίζεται $\text{ind}_{a,p}(b)$.

Βασιζόμενοι σε αυτό το μαθηματικό υπόβαθρο, μπορούμε να ορίσουμε την ανταλλαγή κλειδιών μέσω του Diffie-Helman. Η διαδικασία αυτή χρησιμοποιεί δύο δημόσια γνωστούς αριθμούς, έναν πρώτο αριθμό q και έναν ακέραιο a που είναι πρωτογενής ρίζα του q. Ας υποθέσουμε ότι οι χρήστες A και B επιθυμούν να ανταλλάξουν ένα κλειδί. Ο χρήστης A επιλέγει έναν τυχαίο ακέραιο $X_A < q$ και υπολογίζει τον αριθμό $Y_A = a^{X_A} \bmod q$. Ομοίως, ο χρήστης B επιλέγει έναν τυχαίο ακέραιο $X_B < q$ και υπολογίζει τον αριθμό $Y_B = a^{X_B} \bmod q$. Κάθε ένας από τους χρήστες κρατά τον αντίστοιχο X αριθμό κρυφό και δημοσιοποιεί τον Y. Ο χρήστης A υπολογίζει το κλειδί ως εξής $K = Y_B^{X_A} \bmod q$. Αντίστοιχα, ο χρήστης B υπολογίζει το κλειδί ως εξής $K = Y_A^{X_B} \bmod q$. Οι δύο αυτοί υπολογισμοί οδηγούν στο ίδιο αποτέλεσμα:

$$\begin{aligned}
K &= Y_B^{X_A} \bmod q \\
&= (a^{X_B} \bmod q)^{X_A} \bmod q \\
&= (a^{X_B})^{X_A} \bmod q \\
&= a^{X_B X_A} \bmod q \\
&= (a^{X_A})^{X_B} \bmod q \\
&= (a^{X_A} \bmod q)^{X_B} \bmod q \\
&= Y_A^{X_B} \bmod q.
\end{aligned}$$

Με τον τρόπο αυτό οι δύο πλευρές έχουν καταφέρει να ανταλλάξουν ένα μυστικό κλειδί.

Επιπλέον, επειδή τα X_A και X_B είναι ιδιωτικά, κάθε εισβολέας γνωρίζει μόνο τα q, a, Y_A και Y_B. Προκειμένου να ανακαλύψει το κλειδί, θα πρέπει επομένως να υπολογίσει τον διακριτό λογάριθμο

$$X_B = ind_{a,q}(Y_B).$$

Σε αυτή την περίπτωση, θα μπορέσει να υπολογίσει το κλειδί K με τον ίδιο τρόπο που το υπολόγισε ο χρήστης B.

Η ασφάλεια στην ανταλλαγή κλειδιών με χρήση του Diffie-Helman απορρέει από το γεγονός ότι αν και είναι σχετικά εύκολος ο υπολογισμός εκθετικών εκφράσεων και του υπολοίπου τους με έναν πρώτο αριθμό, είναι εξαιρετικά δύσκολο να υπολογιστούν διακριτοί λογάριθμοι. Για μεγάλους πρώτους αριθμούς, το δεύτερο θεωρείται ακόμη και μη εφικτό.

Στη συνέχεια παρουσιάζεται ένα παράδειγμα. Η ανταλλαγή κλειδιών βασίζεται στη χρήση του πρώτου αριθμού q = 97 και σε μια πρωτογενή ρίζα του 97, στην περίπτωση αυτή a = 5. Οι χρήστες A και B επιλέγουν μυστικά κλειδιά $X_A = 36$ και $X_B = 58$, αντίστοιχα. Καθένας υπολογίζει στη συνέχεια το δημόσιο κλειδί του:

$$Y_A = 5^{36} = 50 \bmod 97$$

$$Y_B = 5^{58} = 44 \bmod 97$$

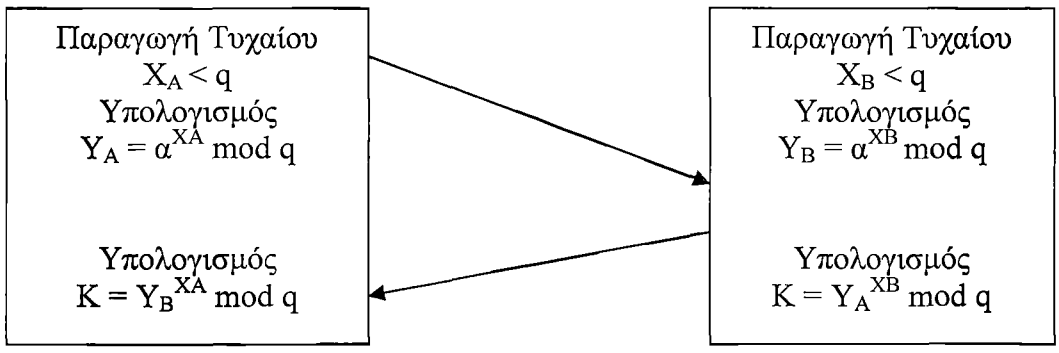
Αφού ανταλλάξουν τα δημόσια κλειδιά τους, ο καθένας υπολογίζει το κοινό μυστικό κλειδί:

$$K = Y_B^{X_A} \bmod q = 44^{36} = 75 \bmod 97$$

$$K = Y_A^{X_B} \bmod q = 50^{58} = 75 \bmod 97$$

Γνωρίζοντας τα {50, 44}, ένας εισβολέας δεν μπορεί εύκολα να υπολογίσει το 75.

Το Σχήμα 11 παρουσιάζει απλό πρωτόκολλο που πραγματοποιεί υπολογισμούς κατά Diffie-Helman. Ας υποθέσουμε ότι ο χρήστης A επιθυμεί να δημιουργήσει μια σύνδεση με το χρήστη B και να χρησιμοποιήσει ένα μυστικό κλειδί για την κρυπτογράφηση μηνυμάτων που αποστέλλονται μέσω αυτής της σύνδεσης. Ο χρήστης A μπορεί να παράγει ένα ιδιωτικό κλειδί μιας χρήσης X_A, να υπολογίσει το Y_A και να το στείλει στο χρήστη B. Ο χρήστης B ανταποκρίνεται δημιουργώντας το δικό του ιδιωτικό κλειδί X_B, υπολογίζοντας το Y_B και στέλνοντάς το στο χρήστη A. Και οι δύο χρήστες μπορούν τώρα να υπολογίσουν το κλειδί. Οι απαραίτητες δημόσια γνωστές τιμές q και a πρέπει να είναι γνωστές εκ των προτέρων. Εναλλακτικά, ο χρήστης A μπορεί να διαλέξει τις τιμές q και a και να τις αποστείλει στον B με το πρώτο του μήνυμα.



Σχήμα 11: Ανταλλαγή Κλειδιών Diffie-Hellman

Ως ένα δεύτερο παράδειγμα χρήσης του Diffie-Helman, ας υποθέσουμε ότι σε μια ομάδα χρηστών (π.χ., χρήστες ένος τοπικού δικτύου), κάθε χρήστης παράγει ένα (μακράς διάρκειας) ιδιωτικό κλειδί X_A και υπολογίζει ένα δημόσιο κλειδί Y_A. Τα δημόσια αυτά κλειδιά, μαζί με

τις δημόσιες τιμές q και a, αποθηκεύονται σε κάποιο βασικό κατάλογο. Οποιαδήποτε χρονική στιγμή, ο χρήστης B μπορεί να προσπελάσει το δημόσιο κλειδί του A, να υπολογίσει ένα ιδιωτικό κλειδί και να το χρησιμοποιήσει για να στείλει ένα κρυπτογραφημένο μήνυμα στο χρήστη A. Αν ο βασικός κατάλογος είναι αξιόπιστος, αυτός ο τύπος επικοινωνίας παρέχει και εμπιστευτικότητα και κάποιου βαθμού πιστοποίηση. Επειδή μόνο οι χρήστες A και B μπορούν να καθορίσουν το κλειδί, κανείς άλλος χρήστης δεν μπορεί να διαβάσει το μήνυμα (εμπιστευτικότητα). Ο παραλήπτης A γνωρίζει ότι μόνο ο χρήστης B μπορεί να έχει δημιουργήσει ένα μήνυμα χρησιμοποιώντας αυτό το κλειδί (πιστοποίηση). Ωστόσο, η τεχνική αυτή, δεν παρέχει προστασία σε επαναλαμβανόμενες επιθέσεις.

2.3 Πιστοποίηση Αυθεντικότητας

Πιστοποίηση αυθεντικότητας είναι η τεχνική με την οποία μια διεργασία πιστοποιεί ότι αυτός με τον οποίο επικοινωνεί είναι αυτός που πρέπει και όχι κάποιος άλλος. Η εξακρίβωση της ταυτότητας μιας απομακρυσμένης διεργασίας είναι αρκετά δύσκολη και απαιτεί σύνθετα πρωτόκολλα βασισμένα στη κρυπτογραφία.

Υπάρχει σύγχυση μεταξύ των εννοιών της πιστοποίησης αυθεντικότητας (authentication) και της εξουσιοδότησης (authorization). Η πιστοποίηση αυθεντικότητας απαντά στην ερώτηση αν πράγματι επικοινωνούμε ή όχι με μια συγκεκριμένη διεργασία, ενώ η εξουσιοδότηση έχει να κάνει με το τι επιτρέπεται να κάνει η διεργασία αυτή. Έτσι, όταν σε έναν εξυπηρέτη ζητείται από μια διεργασία η εκτέλεση μιας εντολής πρέπει, από τη μεριά του εξυπηρέτη, να απαντηθούν οι παρακάτω ερωτήσεις:

1. Η διεργασία αυτή είναι αυτή που ισχυρίζεται ότι είναι (πιστοποίηση αυθεντικότητας);
2. Η διεργασία αυτή επιτρέπεται να εκτελέσει την εντολή αυτή (εξουσιοδότηση);

Μόνο όταν απαντηθούν και οι δύο ερωτήσεις καταφατικά εκτελείται η εντολή. Η πρώτη ερώτηση είναι και η πιο σημαντική. Αν ο εξυπηρέτης γνωρίζει με ποιον επικοινωνεί, τότε ο έλεγχος της εξουσιοδότησης γίνεται με μια απλή αναζήτηση στους τοπικούς πίνακες. Το γενικό μοντέλο που χρησιμοποιούν τα πρωτόκολλα για την πιστοποίηση αυθεντικότητας όταν ένας χρήστης (στην ουσία μια διεργασία) επιθυμεί να εγκαταστήσει μια ασφαλή σύνδεση με ένα δεύτερο χρήστη είναι το ακόλουθο:

1. Ο πρώτος χρήστης ξεκινάει στέλνοντας ένα μήνυμα στο δεύτερο ή σε ένα κέντρο διανομής κλειδιών (key distribution center, KDC) το οποίο είναι αξιόπιστο. Καθώς τα μηνύματα αυτά στέλνονται, ένας εισβολέας μπορεί να υποκλέψει, να τροποποιήσει και να ξαναστείλει τα μηνύματα με σκοπό να παραπλανήσει τους χρήστες. Παρόλα αυτά, όταν το πρωτόκολλο έχει ολοκληρωθεί οι δύο χρήστες είναι σίγουροι ότι μιλάνε ο ένας με τον άλλο.
2. Επιπλέον, στα περισσότερα πρωτόκολλα εγκαθίσταται μεταξύ των δύο χρηστών ένα μυστικό κλειδί συνόδου (session key) για χρήση στην επερχόμενη συνομιλία. Στην πράξη, για λόγους απόδοσης, όλη η κίνηση δεδομένων κρυπτογραφείται χρησιμοποιώντας κρυπτογραφία μυστικού κλειδιού, ενώ η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται στα πρωτόκολλα πιστοποίησης αυθεντικότητας καθώς και για την κρυπτογράφηση των κλειδιών συνόδου. Ο λόγος για τον οποίο χρησιμοποιείται ένα νέο και τυχαία επιλεγμένο κλειδί συνόδου για κάθε νέα σύνδεση είναι η ελαχιστοποίηση της ποσότητας πληροφορίας που διακινείται χρησιμοποιώντας τα δημόσια ή μυστικά κλειδιά των χρηστών. Με τον τρόπο αυτόν επιτυγχάνουμε μείωση της ποσότητας του κρυπτογραφημένου κειμένου που μπορεί να υποκλέψει και να επεξεργαστεί ένας εισβολέας.

2.4 Ψηφιακές Υπογραφές

Η γνησιότητα των περισσότερων νομικών, οικονομικών και άλλων εγγράφων καθορίζεται από την παρουσία ή την απουσία μιας γνήσιας χειρόγραφης υπογραφής. Το ζήτημα της επινόησης ενός υποκατάστατου των χειρόγραφων υπογραφών αποτελεί σημαντικό πρόβλημα. Αυτό που απαιτείται είναι ένα σύστημα μέσω του οποίου μια πλευρά θα μπορεί να στέλνει ένα «υπογεγραμμένο» μήνυμα στην άλλη πλευρά με τέτοιο τρόπο ώστε:

1. Ο παραλήπτης να μπορεί να επιβεβαιώσει την ταυτότητα που δηλώνει ο αποστολέας.
2. Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος.
3. Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

2.4.1 Ο αλγόριθμος Ψηφιακής Υπογραφής DSA (Digital Signature Algorithm)

Ο αλγόριθμος δημοσίου κλειδιού DSA αναπτύχθηκε από το γραφείο Εθνικής Ασφάλειας των ΗΠΑ (NSA) για την παραγωγή ψηφιακών υπογραφών. Το Εθνικό Ινστιτούτο Προτυποποίησης και Τεχνολογίας (NIST) δημοσίευσε αυτό τον αλγόριθμο στο πρότυπο της ψηφιακής υπογραφής (Digital Signature Standard, DSS) ώστε να αποτελέσει το πρότυπο της ψηφιακής πιστοποίησης της Αμερικανικής κυβέρνησης. Η προτυποποίηση του αλγορίθμου έγινε το Μάιο του 1994. Ο αλγόριθμος DSA παρουσιάζεται αναλυτικά στις αναφορές [Δ11, Π03, S96, MOV96].

Ο αλγόριθμος DSA βασίζεται στη δυσκολία υπολογισμού των διακριτών λογαρίθμων. Σε σχέση με τον RSA που μπορεί να χρησιμοποιηθεί τόσο για κρυπτογράφηση όσο και για ψηφιακές υπογραφές, ο DSA μπορεί να εφαρμοστεί μόνο στο χώρο των ψηφιακών υπογραφών.

Στον DSA αρχικά επιλέγονται δύο αριθμοί, p και q. Ο αριθμός p είναι πρώτος αριθμός με μήκος L-bits, όπου ο αριθμός L κυμαίνεται από 512 έως 1024 και είναι ακέραιο πολλαπλάσιο του 64, ενώ ο αριθμός q έχει μήκος 160 bits και είναι ένας πρώτος παράγοντας του αριθμού p-1. Έπειτα, ο αριθμός g υπολογίζεται από τη σχέση:

$$g = h^{(p-1)/q} \bmod p$$

όπου με h παριστάνεται ένας οποιοσδήποτε αριθμός μικρότερος του p-1, έτσι ώστε ο αριθμός g να είναι μεγαλύτερος της μονάδας.

Κατόπιν, επιλέγεται ένας αριθμός x μικρότερος από τον q και υπολογίζεται η παράσταση:

$$y = g^x \bmod p.$$

Οι τρεις παράμετροι p, g και q είναι δημόσια γνωστές. Το δημόσιο κλειδί αποτελεί ο αριθμός x, ενώ το ιδιωτικό κλειδί είναι ο αριθμός y.

Για να υπογραφεί ένα μήνυμα m, επιλέγεται ένας τυχαίος αριθμός K μικρότερος από τον q. Κατόπιν, υπολογίζονται οι αριθμοί r και s από τις παρακάτω σχέσεις:

$$r = (g^K \bmod p) \bmod q$$

$$s = (K^{-1}(H(m)+xr) \bmod q)$$

όπου H(m) είναι μια μονόδρομη συνάρτηση κατακερματισμού (one-way hash function).

Οι μεταβλητές r και s αποτελούν την υπογραφή. Η υπογραφή μπορεί να πιστοποιηθεί υπολογίζοντας τις παρακάτω σχέσεις:

$$w = s^{-1} \bmod q$$

$$u_1 = (H(m)w) \bmod q$$

$$u_2 = (rw) \bmod q$$

$$v = ((g^{u1}y^{u2}) \bmod p) \bmod q$$

Εάν v=r, τότε η υπογραφή είναι έγκυρη.

Η παραγωγή υπογραφών με τον αλγόριθμο DSA γίνεται πολύ πιο γρήγορα σε σχέση με την επαλήθευσή τους. Αντίθετα, στον RSA η επαλήθευση των υπογραφών είναι κατά πολύ γρηγορότερη από την παραγωγή. Πολλοί υποστηρίζουν ότι είναι μεγάλο πλεονέκτημα είναι η δυνατότητα γρήγορης ψηφιακής υπογραφής ενός εγγράφου. Ωστόσο, ένα έγγραφο συνήθως υπογράφεται μόνο μια φορά ενώ χρειάζεται να επαληθεύεται πολλές φορές.

Αν και ο αλγόριθμος DSA έχει επικριθεί αρκετά μετά τη δημοσίευσή του, σήμερα, έχει ενσωματωθεί σε ένα μεγάλο αριθμό συστημάτων και προδιαγραφών. Αξίζει να σημειωθεί ότι η ύπαρξη επικριτικών σχολίων, σε σχέση πάντα με την ασφάλεια, οδήγησε το NIST σε τροποποίηση της αρχικής πρότασης.

2.4.2 Συγχωνεύσεις Μηνυμάτων

Συχνά, η πιστοποίηση αυθεντικότητας είναι απαραίτητη αλλά η μυστικότητα όχι. Εφόσον η κρυπτογραφία είναι μια αργή διαδικασία, είναι συχνά επιθυμητό να είμαστε ικανοί να αποστείλουμε ένα υπογεγραμμένο έγγραφο καθαρού κειμένου. Ένα σχέδιο πιστοποίησης αυθεντικότητας, το οποίο δεν απαιτεί την κρυπτογράφηση ολόκληρου του μηνύματος, βασίζεται στην ιδέα μιας μονόδρομης συνάρτησης κατακερματισμού, η οποία παίρνει ένα αυθαίρετα κομμάτι καθαρού κειμένου και επιστρέφει μια σειρά bits σταθερού μήκους. Η συνάρτηση αυτή που ονομάζεται συγχώνευση μηνύματος (message digest, MD) έχει τρεις βασικές ιδιότητες:

1. Με δεδομένο το καθαρό κείμενο P, είναι εύκολο να υπολογιστεί το MD(P).
2. Με δεδομένο το MD(P), είναι ουσιαστικά απίθανο να βρεθεί το P.
3. Κανείς δεν μπορεί να παράγει δύο μηνύματα που να παρουσιάζουν την ίδια συγχώνευση μηνυμάτων.

Ο υπολογισμός ενός message digest από ένα κομμάτι καθαρού κειμένου είναι αρκετά γρηγορότερος από ότι η κρυπτογράφηση του καθαρού κειμένου με έναν αλγόριθμο δημοσίου κλειδιού. Έτσι, τα message digests μπορούν να χρησιμοποιηθούν ώστε να επιτυγχάνουν τους αλγόριθμους ψηφιακών υπογραφών.

Τα Message digest μπορούν να εφαρμοστούν και στα κρυπτοσυστήματα δημοσίων κλειδιών. Στη περίπτωση αυτή ο χρήστης Α υπολογίζει το message digest από το καθαρό κείμενο που διαθέτει. Στη συνέχεια, ο Α υπογράφει το message digest και στέλνει το υπογεγραμμένο message digest και το καθαρό κείμενο στον Β. Αν τώρα ένας εισβολέας αντικαταστήσει το P κατά τη μετάδοση, ο Β θα το διαπιστώσει όταν θα υπολογίσει το MD(P) από μόνος του.

2.4.3 Συναρτήσεις Κατακερματισμού (Hash Functions)

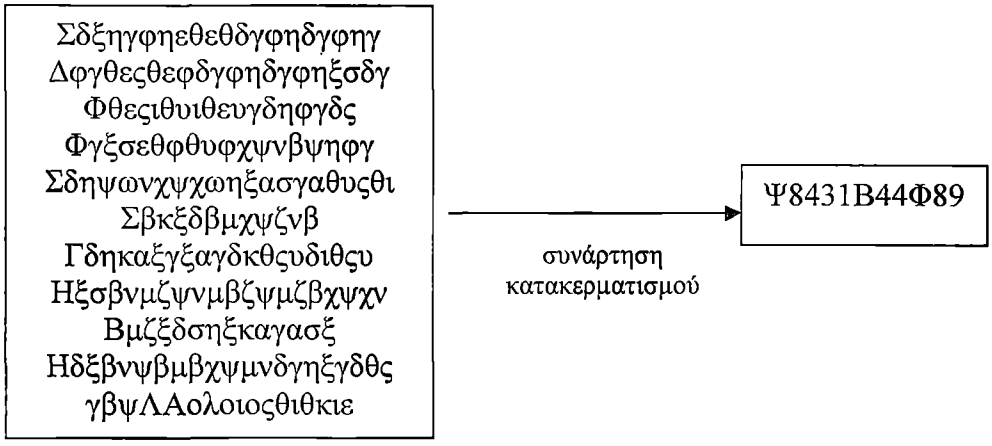
Ο όρος hash function υποδηλώνει ένα μετασχηματισμό (συνάρτηση) που παίρνει ως είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει ως έξοδο μια ακολουθία χαρακτήρων h περιορισμένου μήκους που καλείται hash value, δηλαδή ισχύει h = H(m). Οι συναρτήσεις κατακερματισμού, είναι συναρτήσεις της μορφής H(x) = y, με τις ακόλουθες ιδιότητες:

- Η είσοδος είναι οποιουδήποτε μήκους.
- Η έξοδος έχει συγκεκριμένο μήκος.
- Δεδομένου του x, ο υπολογισμός του y είναι εύκολος.
- Η H(x) είναι μη αντιστρέψιμη.
- Η H(x) είναι αμφιμονοσήμαντη συνάρτηση.

Μια συνάρτηση Η λέμε ότι είναι μη αντιστρέψιμη, αν δοσμένης μιας τιμής κατακερματισμού h είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα m τέτοιο ώστε H(m) = h. Μια

συνάρτηση κατακερματισμού χαρακτηρίζεται ως "ισχυρώς ελεύθερη συγκρούσεων" (strongly collision-free) αν δεν μπορούν να βρεθούν δύο διαφορετικά μηνύματα m_1, m_2 τέτοια ώστε να ισχύει $H(m_1) = H(m_2)$.

Επειδή οι συναρτήσεις κατακερματισμού είναι πιο γρήγορες από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων με την εφαρμογή κρυπτογραφικών διαδικασιών στο συγχωνευμένο μήνυμα, το οποίο είναι πιο μικρό και εύκολο στη διαχείριση. Επιπλέον ένα συγχωνευμένο μήνυμα μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου. Το παραπάνω είναι σημαντικό στις ψηφιακές χρονοσφραγίδες, όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, μπορούν να αποδοθούν χρονοσφραγίδες σε έγγραφα χωρίς να αποκαλυφθεί το περιεχόμενό τους στην υπηρεσία που εκδίδει τις χρονοσφραγίδες.



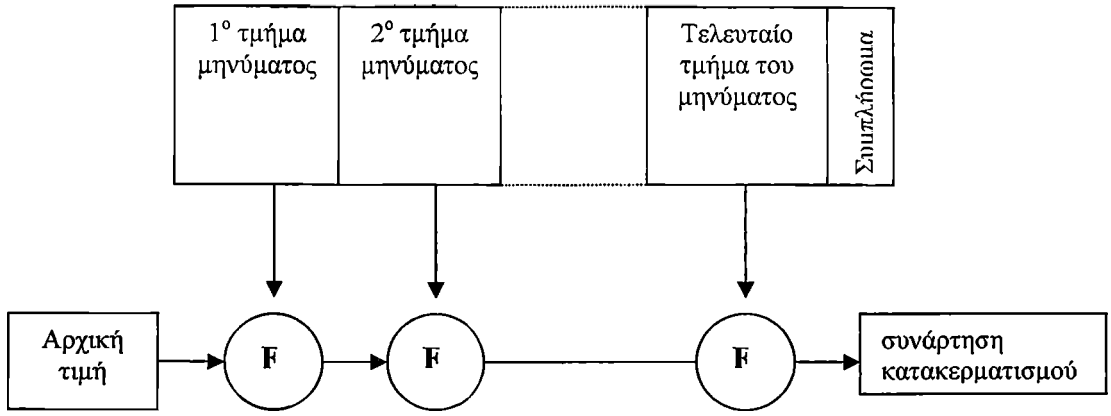
Σχήμα 12: Κρυπτογράφηση με συνάρτηση κατακερματισμού

Οι Damgrad και Merkle επηρέασαν σημαντικά το σχεδιασμό κρυπτογραφικών συναρτήσεων κατακερματισμού εισάγοντας την έννοια της συμπίεσης. Μία συνάρτηση συμπίεσης δέχεται ως είσοδο ένα μήνυμα σταθερού μεγέθους και παράγει στην έξοδο ένα μήνυμα επίσης σταθερού μεγέθους αλλά μικρότερο. Σύμφωνα με τους Damgrad και Merkle, δοσμένης μιας συνάρτησης συμπίεσης, μια συνάρτηση κατακερματισμού μπορεί να οριστεί μέσα από επαναληπτικές εφαρμογές της συνάρτησης συμπίεσης εώς ότου να επεξεργαστεί ολόκληρο το μήνυμα. Σύμφωνα με αυτή τη διαδικασία, ένα μήνυμα αυθαίρετου μεγέθους χωρίζεται σε ομάδες, των οποίων το μέγεθος εξαρτάται από τις προδιαγραφές της συνάρτησης συμπίεσης που χρησιμοποιείται, και συμπληρώνεται (για λόγους ασφαλείας) έτσι ώστε το μέγεθος του μηνύματος να γίνει πολλαπλάσιο του μεγέθους ομάδας. Στη συνέχεια, οι ομάδες επεξεργάζονται σειριακά όπως φαίνεται στο Σχήμα 13 δίνοντας ως έξοδο την τιμή κατακερματισμού για το συγκεκριμένο μήνυμα.

2.4.4 SHA και SHA-1 (Secure Hash Algorithm)

Ο αλγόριθμος SHA, όπως και ο SHA-1, αναπτύχθηκαν από την Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ (NIST) [Π03, S96, MOV96]. Ο SHA-1 αποτελεί επανέκδοση του SHA με διόρθωση μιας ατέλειας του τελευταίου. Ο αλγόριθμος δέχεται ένα μήνυμα μικρότερο των 2^{64} bits σε μέγεθος το οποίο και επεξεργάζεται σε μπλοκ των 512 bits, παράγοντας ένα συγχωνευμένο μήνυμα των 160 bits. Οι αλγόριθμοι αυτοί παρουσιάζονται στις [Δ8, Π03, S96].

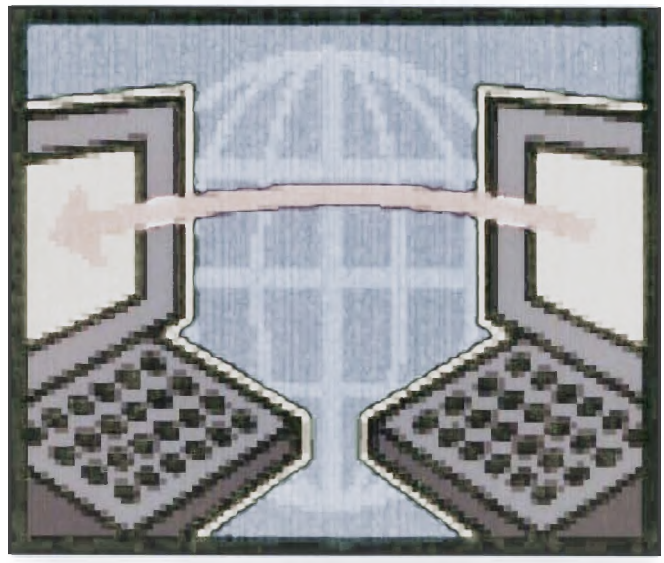
Όσον αφορά τη λειτουργία του, ο αλγόριθμος ξεκινάει διαμορφώνοντας το αρχικό μήνυμα και στη συνέχεια προσθέτει 64 bits για να πάρουμε πολλαπλά μπλοκ των 512 bits. Έπειτα, τοποθετεί μια αρχική τιμή στον καταχωρητή των 160 bits.



Σχήμα 13: Η επαναληπτική δομή Damgrad/Merkle για συναρτήσεις κατακερματισμού, όπου F είναι μια συνάρτηση συμπίεσης.

Για κάθε μπλοκ εισόδου, ο καταχωρητής εξόδου ενημερώνεται χρησιμοποιώντας το μπλοκ των 512 bits εισόδου. Δεν χρησιμοποιείται πίνακας τυχαίων αριθμών (ούτε τιμών συνάρτησης ημιτόνου), αλλά για κάθε μπλοκ υπολογίζονται 80 κύκλοι, επιτυγχάνοντας έτσι μια πολύπλοκη ανάμιξη. Κάθε ομάδα 20 κύκλων χρησιμοποιεί και διαφορετικές συναρτήσεις ανάμιξης.

3 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ



3.1 Εισαγωγή

Το ηλεκτρονικό ταχυδρομείο (e-mail) είναι μία από τις περισσότερο διαδεδομένες εφαρμογές του διαδικτύου. Ίσως το μοναδικό μειονέκτημα που θα μπορούσε να του καταλογίσει κανείς είναι ότι είναι ευάλωτο σε αδιάκριτους εισβολείς. Έτσι ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου δεν διασφαλίζουν το προσωπικό απόρρητο του χρήστη και την ακεραιότητα της λειτουργίας του συστήματος. Για να κατανοηθεί το πώς προσβάλλεται το σύστημα θα περιγράψουμε συνοπτικά τον τρόπο διακίνησης της ηλεκτρονικής αλληλογραφίας.

Κύριος φορέας των μηνυμάτων του ηλεκτρονικού ταχυδρομείου είναι το πρωτόκολλο μεταφοράς απλού ταχυδρομείου. Γνωστά πρωτόκολλα ηλεκρονικού ταχυδρομείου αναφέρονται στη συνέχεια.

SMTP (Simple **M**ail **T**ransfer **P**rotocol): Πρωτόκολλο μεταφοράς απλού ταχυδρομείου.

- Αναλαμβάνει τη μεταφορά των μηνυμάτων από το τερματικό του χρήστη στον εξυπηρέτη (server)
- Αναλαμβάνει τη μεταφορά των μηνυμάτων από έναν εξυπηρέτη σε άλλο.

ISP (Internet Service **P**rovider): Παροχέας υπηρεσιών δικτύου.

- Διαθέτει έναν ή περισσότερους εξυπηρέτες ηλεκτρονικού ταχυδρομείου.
- Υπεύθυνος για αποθήκευση και αποστολή μηνυμάτων.

POP (Post **O**ffice **P**rotocol): Πρωτόκολλο ταχυδρομείου.

IMAP (Internet **M**essage **A**ccess **P**rotocol): Πρωτόκολλο προσπέλασης μηνύματος στο Διαδίκτυο.

Το πρόβλημα της ασφάλειας που προκύπτει είναι το γεγονός ότι τα πακέτα μηνυμάτων είναι προσπελάσιμα από οποιονδήποτε έχει πρόσβαση στο δίκτυο και χρησιμοποιεί ένα εργαλείο ανάλυσης δικτύων (network diagnostics tool ή sniffer). Έτσι δεδομένου ότι με ένα sniffer είναι δυνατή η υποκλοπή (ακόμη και διαφορετικών πρωτοκόλλων) πακέτων που διέρχονται από έναν κόμβο του δικτύου, και ότι οι sniffers είναι διαθέσιμοι στο διαδίκτυο, γίνεται κατανοητός ο κίνδυνος στην ηλεκτρονική αλληλογραφία.

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να αντιμετωπίσει απειλές όπως η πλαστογράφηση, η αλλοίωση του περιεχομένου του, η άρνηση υπηρεσίας και η απόρριψη. Οι υπηρεσίες ασφάλειας του ηλεκτρονικού ταχυδρομείου συνοψίζονται στις ακόλουθες:

1. Εμπιστευτικότητα περιεχομένου.
2. Πιστοποίηση της πηγής ενός μηνύματος.
3. Ακεραιότητα του περιεχομένου.
4. Μη-απόρριψη υποχρέωσης ή οφειλής.

Τα τελευταία χρόνια, τρία βασικά σχήματα έχουν προταθεί για την παροχή υπηρεσιών ασφαλείας στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου:

1. Privacy Enhanced Mail (PEM),
2. Secure MIME (S/MIME),
3. Pretty Good Privacy (PGP).

Αξίζει να σημειωθεί ότι τα σχήματα αυτά παρουσιάζουν περισσότερες ομοιότητες παρά διαφορές. Στη πτυχιακή αυτή θα εστιάσουμε στο σύστημα PGP και θα αναλύσουμε τον τρόπο λειτουργίας του.

3.2 Pretty Good Privacy (PGP)

Το PGP είναι ένα πακέτο δημοσίου-κλειδιού κρυπτογράφησης, που προστατεύει τα e-mail και τα αρχεία δεδομένων. Επιτρέπει την ασφαλή επικοινωνία με ανθρώπους που ποτέ δεν έχουμε συναντήσει μέσα από μη ασφαλή κανάλια. 'Εχει χαρακτηριστεί ως πολύ καλό και ταχύτατο, παρέχει δε σοφιστική διαχείριση των κλειδιών, ψηφιακές υπογραφές, συμπίεση δεδομένων και εργονομική σχεδίαση. Το σύστημα PGP παρουσιάζεται αναλυτικά στις αναφορές [S99, S94, PGP02-1].

Το PGP υπάρχει χάριν στην προσπάθεια ενός ατόμου, του Phil Zimmermann, παρέχει εχεμύθεια και υπηρεσίες πιστοποίησης που μπορούν να χρησιμοποιηθούν στο ηλεκτρονικό ταχυδρομείο και εφαρμογές αποθήκευσης αρχείων. Στην ουσία ο Zimmermann κατάφερε τα παρακάτω:

1. Επέλεξε τους καλύτερους διαθέσιμους κρυπτογραφικούς αλγόριθμους για τη βασική δομή του PGP.

2. Ενσωμάτωσε αυτούς τους αλγόριθμους σε μια εφαρμογή γενικής χρήσεως που είναι ανεξάρτητη από λειτουργικό σύστημα και επεξεργαστή και βασίζεται σε ένα μικρό σύνολο από εύχρηστες εντολές.

3. 'Εκανε το πακέτο και τα σχετικά με αυτό δεδομένα, συμπεριλαμβανομένου και του πηγαίου κώδικα, δωρεάν διαθέσιμο μέσα από το διαδίκτυο, μαζί με πίνακες ενημερώσεως και εμπορικά δίκτυα όπως είναι το 'compuserve'.

4. Συμφώνησε με μια εταιρία, την ViaCrypt -που τώρα είναι δικτυακοί συνεργάτες- για να παρέχει μια πλήρως συμβατή και χαμηλού κόστους εμπορική έκδοση του PGP.

Το PGP έχει επεκταθεί εκρηκτικά και τώρα χρησιμοποιείται ευρύτατα. 'Ενας αριθμός από αιτίες συνδέεται με αυτή την ευρεία αποδοχή του PGP.

1. Διατίθεται δωρεάν σε όλο τον κόσμο σε εκδόσεις που τρέχουν σε μια ποικιλία από πλατφόρμες όπως DOS/WINDOWS, UNIX, MACINTOSH κ.α. Επιπρόσθετα, υπάρχει και η εμπορική έκδοση που ικανοποιεί χρήστες που θέλουν το συγκεκριμένο προϊόν να υποστηρίζεται από τον προμηθευτή.

2. Βασίζεται σε αλγόριθμους δοκιμασμένους σε εκτενή δημόσια χρήση που θεωρούνται πάρα πολύ ασφαλείς. Συγκεκριμένα το πακέτο μεταξύ άλλων περιλαμβάνει:

1 RSA, DSS, Diffie-Hellman, για κωδικοποίηση δημοσίων κλειδιών,

2 IDEA, 3DES, για συμβατική κωδικοποίηση, και

3 SHA-1, για κωδικοποίηση κατακερματισμού.

3. Έχει μια ευρεία ακτίνα εφαρμογών που ξεκινά από εταιρείες που επιθυμούν να επιλέγουν και να ενδυναμώνουν μια τυποποιημένη μέθοδο για την κωδικοποίηση αρχείων και μηνυμάτων, και καταλήγει σε μεμονωμένα άτομα που επιθυμούν να επικοινωνήσουν με ασφάλεια με άλλους σε όλο τον κόσμο μέσω του Διαδικτύου και άλλων δικτύων.

4. Δεν αναπτύχθηκε ούτε ελέγχεται από κανέναν κυβερνητικό ή άλλο οργανισμό προδιαγραφών. Για αυτούς τους οργανισμούς υπάρχει μια στοιχειώδης απιστία ως προς το 'κατεστημένο' κι έτσι το PGP γίνεται πιο ελκυστικό.

Ξεκινάμε με μια συνολική ματιά στη λειτουργία του PGP. Στη συνέχεια εξετάζουμε πως δημιουργούνται τα κλειδιά της κρυπτογράφησης και πως αποθηκεύονται. Κατόπιν αναλύουμε το ζωτικής σημασίας θέμα της διαχείρισης των δημοσίων κλειδιών.

3.2.1 Συμβολογραφία

Στο Σχήμα 14 συνοψίζουμε μια σειρά από νέους συμβολισμούς:

Συμβολισμός	Περιγραφή	
K_S	Session Key	κλειδί συνόδου
KRa	pRivate Key of user A	ιδιωτικό κλειδί του χρήστη Α
KUa	pUblic Key of user A	δημόσιο κλειδί του χρήστη Α
EP	Public key Encryption	κρυπτογράφηση δημοσίου-κλειδιού
DP	Public key Decryption	αποκρυπτογράφηση δημοσίου-κλειδιού
EC	Conventional Encryption	συμβατική κρυπτογράφηση
DC	Conventional Decryption	συμβατική αποκρυπτογράφηση
H	Hash function	συνάρτηση κατακερματισμού
||	Concatenation	συνένωση
Z	Zip algorithm	αλγόριθμος συμπίεσης ZIP
R64	Radix-64 ASCII format	μορφοποίηση σε radix-64 ASCII

Σχήμα 14: Συμβολογραφία του PGP

3.2.2 Περιγραφή λειτουργίας

Η πραγματική λειτουργία του PGP εκπροσωπείται από 5 υπηρεσίες:

- πιστοποίηση
- εμπιστευτικότητα
- συμπίεση
- συμβατότητα ηλεκτρονικού-ταχυδρομείου
- κατάτμηση

Θα εξετάσουμε κάθε μία από αυτές με τη σειρά. Μια περίληψη των υπηρεσιών του PGP παρουσιάζεται στο Σχήμα 15

3.2.2.1 Πιστοποίηση

Το Σχήμα 16(α) απεικονίζει την υπηρεσία της ψηφιακής υπογραφής που παρέχεται από το PGP. Η λειτουργία της εξηγείται με τα παρακάτω βήματα:

1. Ο αποστολέας δημιουργεί ένα μήνυμα.

2. Παράγεται ένας 160-bit κώδικας κατακερματισμού του μηνύματος με τον αλγόριθμο SHA-1.

ΥΠΗΡΕΣΙΕΣ	ΛΕΙΤΟΥΡΓΙΑ	ΑΛΓΟΡΙΘΜΟΣ	ΠΕΡΙΓΡΑΦΗ
Πιστοποίηση	Ψηφιακή υπογραφή	DSS/SHA ή RSA/SHA	Ένας κώδικας κατακερματισμού του μηνύματος δημιουργείται από τον SHA-1. Αυτό το message digest κρυπτογραφείται με τη χρήση του DSS ή RSA μαζί με το ιδιωτικό κλειδί του αποστολέα και συμπεριλαμβάνεται στο μήνυμα.
Εμπιστευτικότητα	Κρυπτογράφηση μηνύματος	IDEA ή 3DES με Diffie-Hellman ή RSA	Το μήνυμα κρυπτογραφείται με χρήση του IDEA ή 3DES, μαζί με ένα μιας χρήσης κλειδί συνόδου (Ks) που παράγεται από τον αποστολέα. Το Ks κρυπτογραφείται με Diffie-Hellman ή RSA με το δημόσιο κλειδί του παραλήπτη και συμπεριλαμβάνεται στο μήνυμα.
Συμπίεση	Συμπίεση	ZIP	Ένα μήνυμα μπορεί να συμπιεστεί, με χρήση ZIP, για αποθήκευση και μεταφορά.
Συμβατότητα ηλεκτρονικού-ταχυδρομείου	Συμβατότητα ηλεκτρονικού-ταχυδρομείου	Radix 64-μετατροπή	Για λόγους διαφάνειας σε εφαρμογές ηλεκτρονικού-ταχυδρομείου, ένα κρυπτογραφημένο μήνυμα θα μπορούσε να μετατραπεί σε ASCII συμβολοσειρά χρησιμοποιώντας Radix-64 μετατροπή.
Κατάτμηση	Κατάτμηση	-	Για να διευθετήσει μέγιστα όρια στο μέγεθος του μηνύματος, το PGP εκτελεί κατάτμηση και επανασυναρμολόγηση

Σχήμα 15: Περίληψη Υπηρεσιών PGP

3. Ο κώδικας κατακερματισμού κρυπτογραφείται με τον αλγόριθμο RSA χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα και το αποτέλεσμα προσκολλάται στην αρχή του μηνύματος.

4. Ο παραλήπτης χρησιμοποιεί τον RSA αλγόριθμο μαζί με το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει και να ανακαλύψει τον κώδικα κατακερματισμού.

5. Ο παραλήπτης παράγει ένα νέο κώδικα κατακερματισμού για το μήνυμα και το συγκρίνει με τον αποκρυπτογραφημένο κώδικα κατακερματισμού. Αν τα παραπάνω ταιριάζουν τότε το μήνυμα γίνεται αποδεκτό ως αυθεντικό.

Ο συνδυασμός των αλγορίθμων SHA-1 και RSA παρέχει ένα αποτελεσματικό σχήμα ψηφιακής υπογραφής. Εξαιτίας της ισχύος του αλγορίθμου RSA, ο παραλήπτης επιβεβαιώνει ότι μόνο ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού, μπορεί να παράγει την ψηφιακή υπογραφή. Εξαιτίας της ισχύος του αλγόριθμου SHA-1, ο παραλήπτης επιβεβαιώνει ότι κανείς άλλος δεν μπορεί να παράγει ένα νέο μήνυμα που να επαληθεύεται από τον κώδικα κατακερματισμού και έτσι προκύπτει η υπογραφή του αυθεντικού μηνύματος.

Εναλλακτικά, οι υπογραφές μπορούν να παραχθούν με χρήση του DSS/SHA-1 αλγορίθμων.

Αν και κανονικά οι υπογραφές βρίσκονται προσκολλημένες στο μήνυμα ή στο αρχείο που υπογράφουν αυτό δεν είναι πάντα ο κανόνας: υποστηρίζονται και μεμονωμένες υπογραφές. Μία μεμονωμένη υπογραφή μπορεί να αποθηκευτεί και να σταλεί ξεχωριστά από το μήνυμα που υπογράφει. Αυτό είναι χρήσιμο σε αρκετές περιπτώσεις. Ένας χρήστης μπορεί να επιθυμεί να διατηρεί ένα ξεχωριστό ημερολόγιο καταγραφής υπογραφών από όλα τα μηνύματα που στέλνει ή λαμβάνει. Μία μεμονωμένη υπογραφή ενός εκτελέσιμου προγράμματος μπορεί να ανιχνεύσει μεταγενέστερη μετάδοση ιού. Τελικά οι μεμονωμένες υπογραφές μπορούν να χρησιμοποιηθούν όταν περισσότερα από ένα άτομα πρέπει να υπογράψουν ένα έγγραφο, όπως είναι ένα νομικό συμβόλαιο. Η υπογραφή του κάθε ατόμου είναι ανεξάρτητη και επομένως εφαρμόζεται μόνο στο έγγραφο. Διαφορετικά, οι υπογραφές θα ήταν φωλιασμένες, με τον δεύτερο υπογράφοντα να υπογράφει το έγγραφο που περιέχει και την υπογραφή του πρώτου, και ούτω καθ' εξής.

3.2.2.2 Εμπιστευτικότητα

Μια άλλη βασική υπηρεσία που υποστηρίζεται από το PGP είναι η εμπιστευτικότητα, η οποία παρέχεται από κρυπτογραφημένα μηνύματα που θα μεταδοθούν ή θα αποθηκευτούν τοπικά ως αρχεία. Και στις δύο περιπτώσεις ο αλγόριθμος της συμβατικής κρυπτογραφίας IDEA ή ο 3-DES ή CAST-128 μπορεί να χρησιμοποιηθεί.

Θα αναφερθούμε τώρα στο πρόβλημα της διανομής των κλειδιών. Στο PGP κάθε συμβατικό κλειδί χρησιμοποιείται μόνο μία φορά. Έτσι, ένα νέο κλειδί, που ονομάζεται κλειδί συνόδου, παράγεται από έναν τυχαίο 128-bit αριθμό για κάθε μήνυμα. Επειδή θα χρησιμοποιηθεί μόνο μία φορά, το κλειδί συνόδου τοποθετείται στο μήνυμα και εκπέμπεται μαζί με αυτό. Για την προστασία του, το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη. Το Σχήμα 16(β) απεικονίζει αυτή τη διαδικασία η οποία μπορεί να περιγραφεί ως εξής:

1. Ο αποστολέας παράγει το μήνυμα και έναν τυχαίο 128-bit αριθμό που προορίζεται να χρησιμοποιηθεί σαν κλειδί συνόδου για αυτό το μήνυμα.

2. Το μήνυμα κρυπτογραφείται με τον αλγόριθμο IDEA ή 3DES ή CAST-128 χρησιμοποιώντας το κλειδί συνόδου.

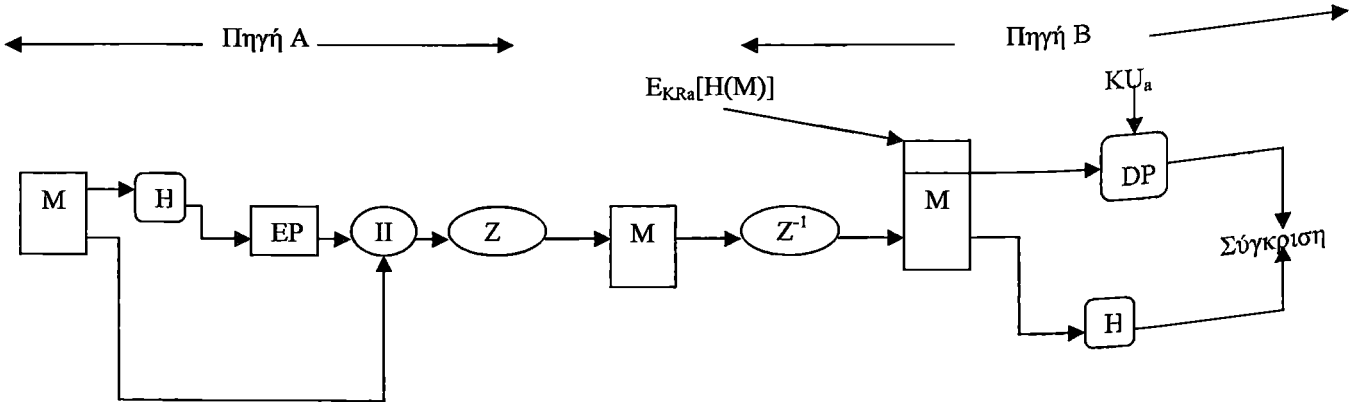
3. Το κλειδί συνόδου κρυπτογραφείται με τον αλγόριθμο RSA, χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη και προσκολλάται στο μήνυμα.

4. Ο παραλήπτης χρησιμοποιεί τον αλγόριθμο RSA και το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει και να ανακαλύψει το κλειδί συνόδου.

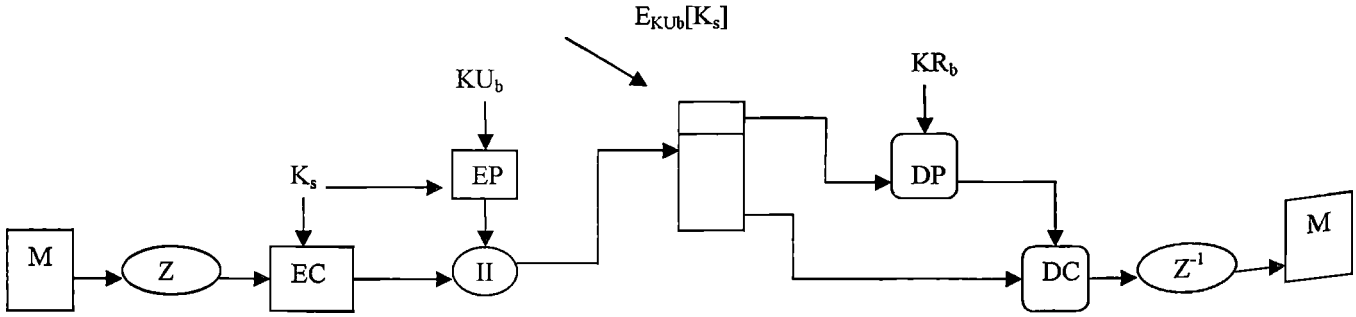
5. Το κλειδί συνόδου χρησιμοποιείται για την αποκρυπτογράφηση του μηνύματος.

Στην χρήση του αλγόριθμου RSA για την κρυπτογράφηση του κλειδιού, το PGP παρέχει εναλλακτικά τη δυνατότητα επιλογής άλλων αλγορίθμων μεταξύ των οποίων και του *Diffie-Hellman.* Αρκετές παρατηρήσεις μπορούν να γίνουν:

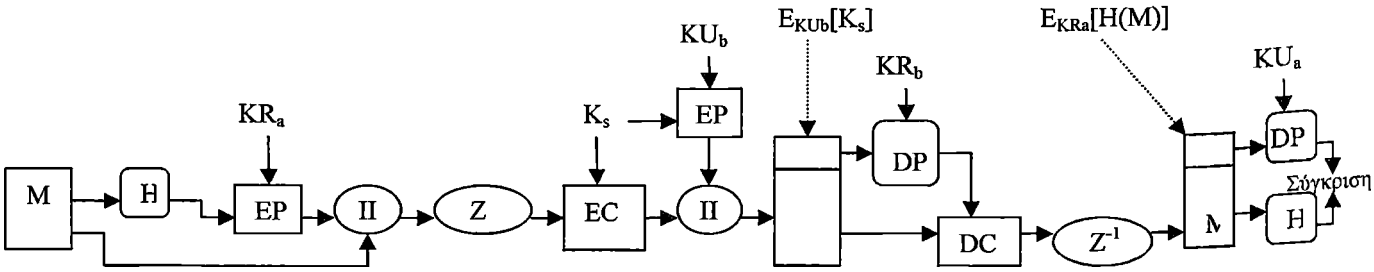
- Για να μειώσουμε το χρόνο κρυπτογράφησης εφαρμόζουμε το συνδυασμό της συμβατικής και δημοσίου-κλειδιού κρυπτογράφησης, σε αντίθεση με την απλή χρήση του RSA ή του Diffie-Helman για την απευθείας κρυπτογράφηση του μηνύματος. Οι συμβατικοί αλγόριθμοι είναι σημαντικά ταχύτεροι από τους RSA και Diffie-Helman.



(α) μπλοκ διάγραμμα πιστοποίησης



(β) μπλοκ διάγραμμα εμπιστευτικότητας



(γ) μπλοκ διάγραμμα εμπιστευτικότητας και πιστοποίησης

Σχήμα 16: Λειτουργίες κρυπτογράφησης του PGP

• Η χρήση του αλγόριθμου δημοσίου-κλειδιού λύνει το πρόβλημα της διανομής του κλειδιού συνόδου, γιατί μόνο ο παραλήπτης είναι σε θέση να ανακαλύψει το κλειδί συνόδου που είναι δεσμευμένο στο μήνυμα. Έτσι δεν απαιτείται κάποιο πρωτόκολλο διανομής του κλειδιού-συνόδου. Ειδικότερα, κάθε μήνυμα είναι ανεξάρτητο γεγονός με το δικό του μιας-χρήσης κλειδί. Επιπρόσθετα, δεδομένου της μορφής της αποθήκευσης και προώθησης του ηλεκτρονικού-ταχυδρομείου, η χρήση της τεχνικής handshaking (χειραψίας) για να εξασφαλίσουμε ότι και οι δύο πλευρές έχουν το ίδιο κλειδί-συνόδου δεν είναι πρακτική. Τελικά η χρησιμοποίηση της μιας-χρήσης συμβατικών κλειδιών, ενισχύει την ήδη ισχυρή προσέγγιση της συμβατικής κρυπτογραφίας. Μόνο μία μικρή ποσότητα του απλού κειμένου κρυπτογραφείται με κάθε κλειδί, χωρίς να υπάρχει σχέση ανάμεσα στα κλειδιά. Έτσι, στο βαθμό που ο αλγόριθμος δημοσίου-κλειδιού είναι ασφαλής, το όλο σύστημα είναι ασφαλές.

3.2.2.3 Εμπιστευτικότητα και Πιστοποίηση

Όπως φαίνεται στο Σχήμα 16(γ), και οι δύο υπηρεσίες, πιστοποίηση και αυθεντικότητα, μπορούν να χρησιμοποιηθούν για το ίδιο μήνυμα. Αρχικά, παράγεται μια ψηφιακή υπογραφή για το μήνυμα του απλού κειμένου και προσκολλάται στην αρχή του μηνύματος. Στη συνέχεια, το μήνυμα του απλού κειμένου κρυπτογραφείται με τον αλγόριθμο IDEA ή τον 3-DES ή τον CAST-128 και ένα κλειδί συνόδου κρυπτογραφείται με τον αλγόριθμο RSA ή τον Diffie-Hellman. Αυτή η ακολουθία βημάτων είναι προτιμότερη από την αντίστροφη, δηλαδή από το να κρυπτογραφηθεί πρώτα το μήνυμα και μετά να παραχθεί μια υπογραφή για το κρυπτογραφημένο πλέον μήνυμα. Είναι γενικότερα πιο βολικό να αποθηκεύεται η υπογραφή με την έκδοση απλού κειμένου του μηνύματος. Επιπλέον, σε περιπτώσεις που εμπλέκεται κάποιο τρίτο πρόσωπο, αυτό δεν χρειάζεται να ασχοληθεί με το συμβατικό κλειδί για την επαλήθευση της υπογραφής.

Συνοπτικά, όταν χρησιμοποιούνται ταυτόχρονα και οι δύο υπηρεσίες, ο αποστολέας υπογράφει πρώτα το μήνυμα με το ιδιωτικό του κλειδί, στη συνέχεια κρυπτογραφεί το μήνυμα με το κλειδί συνόδου και τέλος κρυπτογραφεί το κλειδί συνόδου με το δημόσιο κλειδί του παραλήπτη.

3.2.2.4 Συμπίεση

Το PGP συμπιέζει το μήνυμα μετά την εφαρμογή της υπογραφής και πριν την κρυπτογράφηση. Αυτό δίνει το πλεονέκτημα της οικονομίας χώρου τόσο για την εκπομπή του μηνύματος, όσο και για την αποθήκευση αρχείων.

Η τοποθέτηση των αλγορίθμων συμπίεσης, που απεικονίζεται με Z για συμπίεση και Z^{-1} για αποσυμπίεση στα Σχήματα 16(α), 16(β) και 16(γ) είναι κρίσιμη:

1. Η υπογραφή παράγεται πριν την συμπίεση για δύο λόγους:

i. Είναι προτιμότερο να υπογράψεις ένα ασυμπίεστο μήνυμα, έτσι ώστε κάποιος να μπορεί να αποθηκεύει μόνο το ασυμπίεστο μήνυμα και την υπογραφή για μελλοντική επαλήθευση. Αν κάποιος υπογράψει ένα συμπιεσμένο έγγραφο, τότε θα ήταν απαραίτητο είτε να αποθηκευτεί η συμπιεσμένη έκδοση του μηνύματος για μεταγενέστερη επαλήθευση, ή να επανασυμπιεστεί το μήνυμα όταν απαιτείται η επαλήθευσή του.

ii. Ακόμη και αν κάποιος ήταν πρόθυμος να παράγει δυναμικά μια επανα-συμπιεσμένη έκδοση του μηνύματος για επαλήθευση, ο αλγόριθμος συμπίεσης του PGP παρουσιάζει μια δυσκολία. Ο αλγόριθμος δεν είναι ντετερμινιστικός. Παρέχεται ποικιλία υλοποιήσεων του αλγορίθμου που επιτυγχάνει διαφορετικές αναλογίες στη σχέση ταχύτητα εκτέλεσης/συμπίεση και σαν αποτέλεσμα παράγονται διαφορετικοί τύποι συμπίεσης. Ωστόσο, αυτοί οι διαφορετικοί τύποι αλγορίθμων είναι διαλειτουργικοί όσον αφορά τη συμπίεση, γιατί κάθε έκδοση του αλγορίθμου μπορεί σωστά να αποσυμπιέσει την έξοδο της οποιασδήποτε έκδοσης. Εφαρμόζοντας τη συνάρτηση κατακερματισμού και την υπογραφή μετά τη συμπίεση θα πρέπει να περιορίσουμε όλες τις εφαρμογές του PGP στον ίδιο αλγόριθμο συμπίεσης.

2. Η κρυπτογράφηση μηνύματος εφαρμόζεται μετά από τη συμπίεση για να ενισχύσει την κρυπτογραφική ασφάλεια. Επειδή το συμπιεσμένο μήνυμα έχει μικρότερο πλεονασμό από το πρωτότυπο κείμενο, η κρυπτανάλυση γίνεται πιο δύσκολη.

Ο αλγόριθμος συμπίεσης που χρησιμοποιείται είναι ο ZIP.

3.2.2.5 Συμβατότητα με Ηλεκτρονικό Ταχυδρομείο

Όταν χρησιμοποιείται το PGP, τουλάχιστον ένα μέρος των δεδομένων που θα αποσταλλούν είναι κρυπτογραφημένο. Στην περίπτωση που χρησιμοποιείται η υπηρεσία υπογραφής, τότε μόνο το message digest κρυπτογραφείται (με το ιδιωτικό κλειδί του αποστολέα). Αν ωστόσο χρησιμοποιείται η υπηρεσία πιστοποίησης, κρυπτογραφείται και το μήνυμα και η υπογραφή

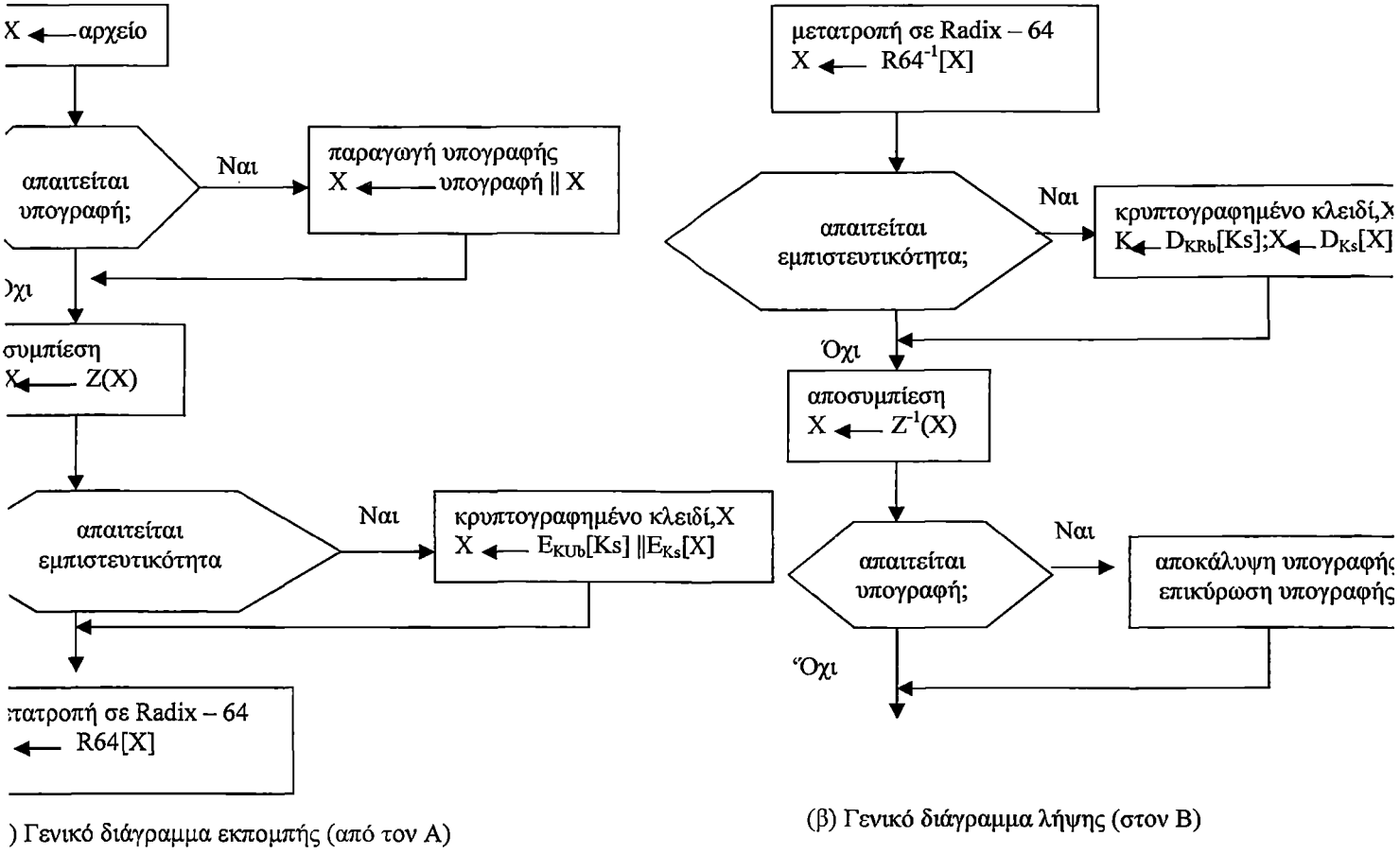
(αν η τελευταία υπάρχει) με ένα συμμετρικό κλειδί μιας χρήσεως. Επομένως, μέρος του μηνύματος ή όλο το μήνυμα αποτελείται από μια ακολουθία αυθαίρετων οκτάδων (8-bits). Ωστόσο, πολλά συστήματα ηλεκτρονικού ταχυδρομείου επιτρέπουν μόνο μηνύματα κειμένου που έχουν κωδικοποιηθεί βάσει του κώδικα ASCII. Προκειμένου τέτοια συστήματα να μπορούν να επεξεργαστούν PGP μηνύματα, το PGP παρέχει μια υπηρεσία μετατροπής της ακατέργαστης 8-bit δυαδικής ροής σε μια ροή εκτυπώσιμων χαρακτήρων ASCII.

Για το σκοπό αυτό γίνεται μετατροπή βάσει του αλγορίθμου μετατροπής Radix-64. Κάθε ομάδα των τριών οκτάδων δυαδικών δεδομένων απεικονίζεται σε τέσσερις χαρακτήρες ASCII. Αυτή η μορφοποίηση προσθέτει επίσης μερικά bits (CRC) προκειμένου να είναι δυνατό να προσδιοριστούν λάθη μετάδοσης. Η χρήση του Radix-64 μεγαλώνει το μήνυμα κατά 33%. Ευτυχώς, τα μέρη του μηνύματος που αποτελούν το κλειδί συνόδου και την υπογραφή είναι σχετικά συμπαγή, ενώ το μήνυμα απλού κειμένου έχει υποστεί συμπίεση. Στην πράξη, η συμπίεση είναι υπεραρκετή για να αντιμετωπίσει την επέκταση αυτή του μηνύματος λόγω του Radix-64. Για παράδειγμα, το μέσο κλάσμα συμπίεσης είναι 2.0 όταν χρησιμοποιείται το ZIP. Αν αγνοήσουμε το μέγεθος της σχετικά μικρής υπογραφής και του κλειδιού, η συνολική επίδραση της συμπίεσης και της επέκτασης που αναφέρθηκαν παραπάνω σε ένα αρχείο μεγέθους X είναι 1.33 * 0.5 * X = 0.655 * X. Επομένως, εξακολουθεί να υφίσταται συμπίεση της τάξης του 1/3.

Είναι αξιοσημείωτο ότι ο αλγόριθμος Radix-64 μετατρέπει αυτόματα τη ροή εισόδου, ανεξάρτητα από τα περιεχόμενα, με σταθερό ρυθμό ακόμη και αν τα εισαγόμενα δεδομένα είναι σε μορφή ASCII. Έτσι, αν το μήνυμα υπογράφεται αλλά δεν κρυπτογραφείται και η μετατροπή εφαρμόζεται σε ολόκληρο το τμήμα, η έξοδος θα είναι δυσανάγνωστη από έναν απλό παρατηρητή, γεγονός το οποίο παρέχει ένα συγκεκριμένο επίπεδο εμπιστευτικότητας. Ως προνόμιο, το PGP μπορεί να διαμορφωθεί ώστε να μετατρέπει σε μορφοποίηση Radix-64 μόνο το τμήμα της υπογραφής των υπογεγραμμένων μηνυμάτων απλού κειμένου. Αυτό επιτρέπει στον παραλήπτη να διαβάσει το μήνυμα χωρίς τη χρήση του PGP. Το PGP μπορεί επίσης να χρησιμοποιηθεί για να επαληθεύει την υπογραφή.

Το Σχήμα 17 δείχνει τη σχέση ανάμεσα στις τέσσερις υπηρεσίες που αναλύσαμε. Κατά την εκπομπή, αν αυτό απαιτείται, μία υπογραφή παράγεται χρησιμοποιώντας ένα κώδικα κατακερματισμού του συμπιεσμένου απλού κειμένου. Τότε το απλό κείμενο και επιπλέον η υπογραφή αν υπάρχει συμπιέζονται. Στη συνέχεια, αν απαιτείται εμπιστευτικότητα, το αποτέλεσμα της συμπίεσης κρυπτογραφείται με ένα κλειδί συνόδου, το οποίο κρυπτογραφείται με τη σειρά του με το δημόσιο κλειδί του αποστολέα και προσκολλάται στην αρχή του μηνύματος. Τελικά, όλο αυτό το πακέτο μετατρέπεται χρησιμοποιώντας τη Radix-64.

Το εισερχόμενο πακέτο ξαναμετατρέπεται στον παραλήπτη από Radix-64 σε δυαδική μορφή. Τότε, αν το μήνυμα είναι κρυπτογραφημένο, ο παραλήπτης αποκρυπτογραφεί το κλειδί-συνόδου και με αυτό αποκρυπτογραφεί στη συνέχεια το μήνυμα. Το αποτέλεσμα που προκύπτει αποσυμπιέζεται. Αν το μήνυμα είναι υπογεγραμμένο, ο παραλήπτης ανακαλύπτει τον κώδικα κατακερματισμού και το συγκρίνει με τον κώδικα κατακερματισμού που υπολογίζει ο ίδιος.



) Γενικό διάγραμμα εκπομπής (από τον A)

(β) Γενικό διάγραμμα λήψης (στον B)

Σχήμα 17: Εκπομπή και λήψη μηνύματος από το PGP.

3.2.2.6 Κατάτμηση και επανασυναρμολόγηση

Οι δραστηριότητες του ηλεκτρονικού-ταχυδρομείου περιορίζονται σε ένα μέγιστο μήκος μηνύματος. Για παράδειγμα αρκετές από τις προσπελάσιμες διαμέσου του Διαδικτύου δραστηριότητες, απαιτούν ένα μέγιστο μήκος από 50000 οκτέτες. Κάθε μεγαλύτερο μήνυμα πρέπει να τεμαχιστεί σε μικρότερα τμήματα, κάθε ένα από τα οποία στέλνεται ξεχωριστά.

Για να προσαρμόσουμε αυτό τον περιορισμό, το PGP αυτόματα υποδιαιρεί ένα μήνυμα που είναι αρκετά μεγάλο σε τμήματα κατάλληλου μεγέθους για να σταλθούν με ηλεκτρονικό ταχυδρομείο. Η κατάτμηση συμβαίνει μετά από όλες τις άλλες διεργασίες, συμπεριλαμβανομένου και της μετατροπής Radix-64. Έτσι το κλειδί συνόδου και η υπογραφή εμφανίζονται μόνο μία φορά, στην αρχή του πρώτου τμήματος. Τέλος, κατά τη λήψη, το PGP πρέπει να απαλλαχθεί από όλες τις προστιθέμενες επικεφαλίδες και να επανασυναρμολογήσει το αυθεντικό πακέτο πριν εκτελεστούν τα βήματα που απεικονίζονται στο Σχήμα 17(β).

3.2.2.7 Κρυπτογραφικά Κλειδιά και Λίστες Κλειδιών

Το PGP κάνει χρήση τεσσάρων τύπων κλειδιών:

- μιας χρήσης συμβατικών κλειδιών συνόδου,
- δημοσίων κλειδιών,

- ιδιωτικών κλειδιών,
- συμβατικών κλειδιών κωδικού πρόσβασης (εξηγούνται παρακάτω).

Τρεις διαφορετικές προδιαγραφές μπορούν να ταυτοποιήσουν αυτά τα κλειδιά:

1. Απαιτείται μια διαδικασία παραγωγής απρόβλεπτων κλειδιών-συνόδων.

2. Θα ήταν θεμιτό να επιτραπεί στο χρήστη να έχει πολλαπλά ζεύγη δημοσίου/ιδιωτικού κλειδιού. Ένας λόγος είναι ότι μπορεί να επιθυμεί να αλλάζει το ζεύγος κλειδιών του, από καιρό σε καιρό. Όταν αυτό συμβαίνει, τα καθ' οδόν μηνύματα θα κατασκευαστούν με το παλιό κλειδί. Επιπρόσθετα, οι παραλήπτες θα γνωρίζουν μόνο το παλιό δημόσιο κλειδί μέχρι μια ενημέρωση να φτάσει σε αυτούς. Μαζί με την ανάγκη αλλαγής των κλειδιών με τη πάροδο του χρόνου, ένας χρήστης μπορεί να επιθυμεί να έχει πολλαπλά ζεύγη κλειδιών σε μια δεδομένη στιγμή για να επικοινωνεί με διαφορετικές ομάδες από αλληλογράφους ή απλά να αυξήσει την ασφάλεια με περιορισμό της ποσότητας του κρυπτογραφημένου υλικού με ένα κλειδί. Το συμπέρασμα όλων αυτών είναι ότι δεν υπάρχει μία προς μία αντιστοίχιση ανάμεσα στους χρήστες και τα δημόσια κλειδιά τους. Έτσι, απαιτούνται διαδικασίες για την ταυτοποίηση των ειδικών κλειδιών.

3. Κάθε περιβάλλον PGP πρέπει να διατηρεί ένα αρχείο από τα δικά του ζεύγη δημόσιου/ιδιωτικού κλειδιών καθώς επίσης και ένα αρχείο των δημοσίων κλειδιών των αλληλογράφων.

Εξετάζουμε κάθε μία από αυτές τις απαιτήσεις με τη σειρά.

Παραγωγή κλειδιού-συνόδου

Κάθε κλειδί συνόδου είναι συνδυασμένο με ένα απλό μήνυμα και χρησιμοποιείται με σκοπό την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος. Υπενθυμίζουμε ότι η κρυπτογράφηση/αποκρυπτογράφηση μηνύματος γίνεται με ένα συμμετρικό αλγόριθμο κρυπτογράφησης. Οι IDEA και CAST-128 χρησιμοποιούν 128-bit κλειδιά. Ο 3-DES χρησιμοποιεί 168-bit κλειδί. Για την περιγραφή που ακολουθεί κάνουμε την παραδοχή του CAST-128.

Ο CAST-128 παράγει τυχαίους αριθμούς των 128-bit. Η είσοδος της γεννήτριας τυχαίων αριθμών αποτελείται από ένα 128-bit κλειδί και δύο δεσμευμένα 64-bit μπλοκ που ο χειρισμός τους γίνεται ως απλό κείμενο που θα κρυπτογραφηθεί. Χρησιμοποιώντας τη μέθοδο της ανάδρασης κρυπτογραφήματος (CFB, Cipher FeedBack), ο CAST-128 παράγει δύο 64-bit δεσμευμένα μπλοκ κρυπτογραφημένου κειμένου, τα οποία συνενώνονται για να δημιουργήσουν το 128-bit κλειδί συνόδου.

Η είσοδος απλού κειμένου στη γεννήτρια τυχαίων αριθμών, αποτελείται από δύο 64-bit δεσμευμένα μπλοκ που παράγονται αυτόνομα από μία ροή τυχαίων 128-bit αριθμών. Αυτοί οι αριθμοί προέρχονται από τυχαία πληκτρολόγηση. Η τυχαία ακολουθία αριθμών συνδυάζεται με την έξοδο του προηγούμενου κλειδιού συνόδου από τον CAST-128 και διαμορφώνει την είσοδο του κλειδιού προς τη γεννήτρια. Το αποτέλεσμα είναι να παραχθεί μία ακολουθία από απρόβλεπτα και αποτελεσματικά κλειδιά συνόδου.

Αναγνωριστικά κλειδιών

Όπως προαναφέραμε, ένα κρυπτογραφημένο μήνυμα συνοδεύεται από μια κρυπτογραφημένη μορφή του κλειδιού συνόδου. Το κλειδί συνόδου κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη. Ως εκ τούτου, μόνο ο παραλήπτης είναι σε θέση να ανακαλύψει το κλειδί συνόδου και επομένως και το μήνυμα. Αν κάθε χρήστης χρησιμοποιεί ένα μοναδικό ζεύγος δημοσίου/ιδιωτικού κλειδιού, τότε ο παραλήπτης θα μπορούσε αυτόματα να γνωρίζει ποιο κλειδί να χρησιμοποιήσει για να αποκρυπτογραφήσει το κλειδί συνόδου: το μοναδικό ιδιωτικό κλειδί του. Όμως έχει συζητηθεί η προδιαγραφή κάθε χρήστης να μπορεί να χρησιμοποιεί πολλαπλά ζεύγη δημόσιου/ιδιωτικού κλειδιού.

Δημιουργείται επομένως το ερώτημα πως μπορεί ο παραλήπτης να γνωρίζει ποιο από τα δημόσια κλειδιά χρησιμοποιήθηκε για την κρυπτογράφηση του κλειδιού συνόδου. Μια απλή λύση θα μπορούσε να είναι η αποστολή του δημοσίου κλειδιού μαζί με το μήνυμα. Ο παραλήπτης μπορεί τότε να επικυρώσει ότι όντως αυτό είναι ένα από τα δημόσια κλειδιά και να συνεχίσει. Παρότι αυτό το σχέδιο θα μπορούσε να δουλέψει, παρουσιάζει ανώφελη σπατάλη χώρου. Ένα δημόσιο κλειδί του αλγόριθμου RSA μπορεί να έχει μήκος εκατοντάδων δεκαδικών ψηφίων. Μια άλλη λύση θα μπορούσε να είναι η συσχέτιση ενός αναγνωριστικού (identifier), μοναδικού στο χώρο κάθε χρήστη, με κάθε δημόσιο κλειδί. Αυτό σημαίνει ότι ο συνδυασμός του αναγνωριστικού χρήστη και του αναγνωριστικού κλειδιού θα μπορούσε να είναι επαρκής για την ταυτοποίηση ενός μοναδικού κλειδιού. Τότε, μόνο το αναγνωριστικό κλειδιού (που είναι μικρότερου μεγέθους) θα χρειαζόταν να αποσταλεί. Αυτή η λύση ωστόσο προκαλεί ένα μεγάλο πρόβλημα διαχείρισης: τα αναγνωριστικά κλειδιών πρέπει να προσδιοριστούν και να αποθηκευτούν με τέτοιο τρόπο ώστε και ο αποστολέας και ο παραλήπτης να μπορούν από το αναγνωριστικό να χαρτογραφήσουν το δημόσιο κλειδί. Αυτό μοιάζει να είναι ενοχλητικά περίπλοκο.

Η λύση που εφαρμόζεται από το PGP είναι η συσχέτιση ένος αναγνωριστικού κλειδιού (key-ID) για κάθε δημόσιο κλειδί, το οποίο είναι με πολύ μεγάλη πιθανότητα μοναδικό στο χώρο κάθε χρήστη. Το αναγνωριστικό αυτό σε συνδυασμό με κάθε δημόσιο κλειδί αποτελείται από τα τελευταία 64 σημαντικά bits του κλειδιού. Αυτό σημαίνει ότι το key-ID του δημοσίου κλειδιού KU_a είναι (KU_a mod 2^{64}). Αυτό είναι ένα κατάλληλο μήκος τέτοιο ώστε η πιθανότητα της αναπαραγωγής του key-ID να είναι πολύ μικρή.

Ένα key-ID απαιτείται επίσης για τις ψηφιακές υπογραφές του PGP. Επειδή ένας αποστολέας μπορεί να χρησιμοποιήσει μόνο ένα από έναν αριθμό ιδιωτικών κλειδιών για να κρυπτογραφήσει το messsage digest, ο παραλήπτης πρέπει να γνωρίζει ποιο δημόσιο κλειδί προορίζεται για χρήση. Άρα, τα συστατικά της ψηφιακής υπογραφής ενός μηνύματος περιλαμβάνουν το 64-bit key-ID από το απαιτούμενο δημόσιο κλειδί. Όταν το μήνυμα λαμβάνεται, ο παραλήπτης επικυρώνει ότι το key-ID αναφερέται σε ένα δημόσιο κλειδί που γνωρίζει για τον αποστολέα και τότε προχωρά στην επικύρωση της υπογραφής.

Τώρα που η έννοια του key-ID έχει περιγραφεί, μπορούμε να πάρουμε μια πιο λεπτομερή άποψη για τη μορφοποίηση ενός εκπεμπόμενου μηνύματος, η οποία απεικονίζεται στο Σχήμα 18. Ένα μήνυμα αποτελείται από τρία συστατικά:

1. το τμήμα μηνύματος,

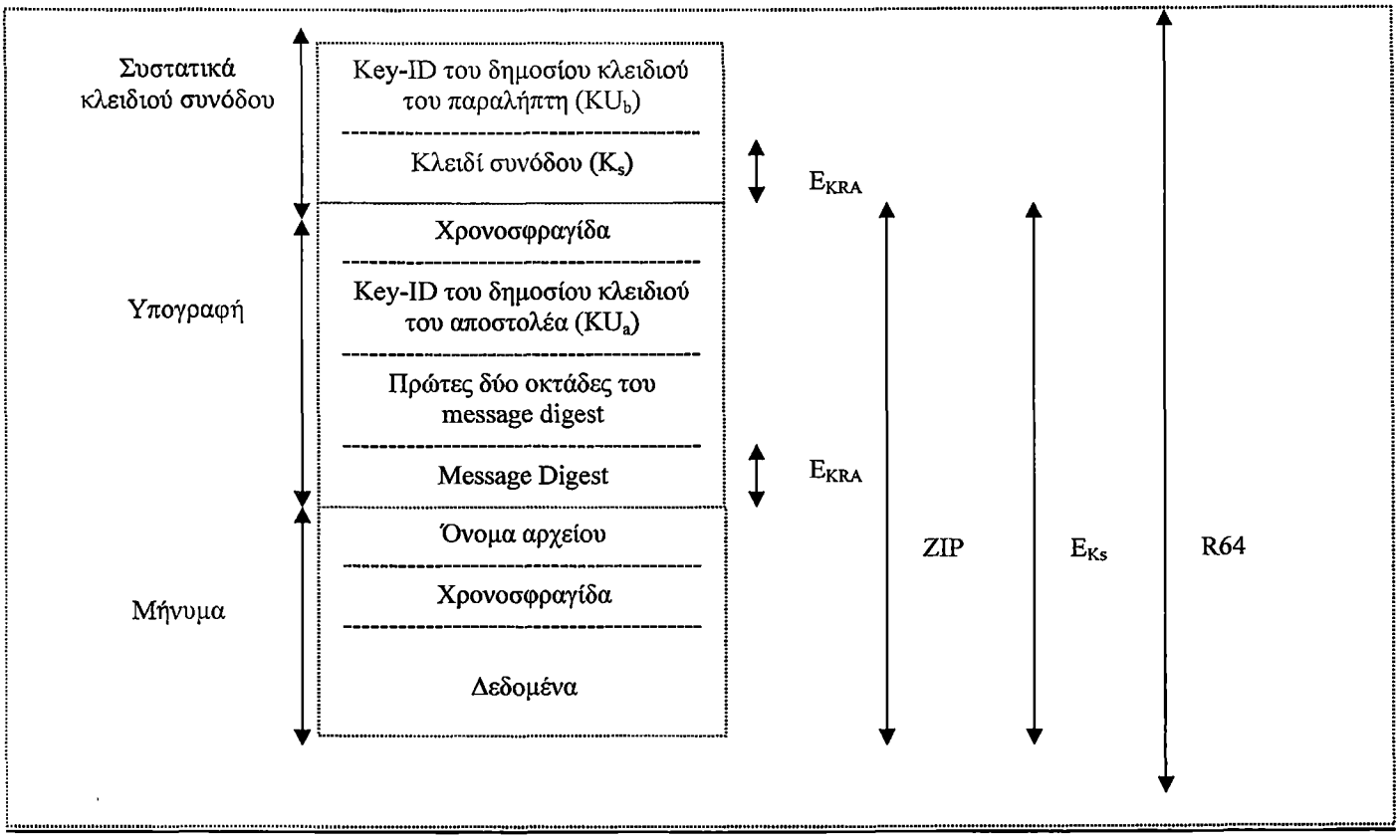
2. μία υπογραφή (προαιρετική),

3. ένα κλειδί συνόδου (προαιρετικό).

Το **τμήμα μηνύματος** περιλαμβάνει τα πραγματικά προς αποθήκευση ή προς αποστολή δεδομένα, καθώς επίσης ένα όνομα του αρχείου και μία χρονοσφραγίδα που καθορίζει το χρόνο δημιουργίας του.

Το **τμήμα υπογραφής** περιλαμβάνει τα ακόλουθα:

- **Χρονοσφραγίδα:** Η χρονική στιγμή στην οποία δημιουργήθηκε η υπογραφή.



Συμβολισμοί:

E_{KUb} = κρυπτογράφηση με ιδιωτικό κλειδί του χρήστη b

E_{KRa} = κρυπτογράφηση με δημόσιο κλειδί του χρήστη a

E_{Ks} = κρυπτογράφηση με κλειδί συνόδου

ZIP = συνάρτηση συμπίεσης Zip

R-64 = συνάρτηση μετατροπής Radix-64

Σχήμα 18: Γενική μορφοποίηση μηνύματος από το PGP (από τον A στο B)

- **Message digest**: Ο 160-bit SHA-1 κώδικας κατακερματισμού, κρυπτογραφημένος με το ιδιωτικό κλειδί του αποστολέα. Το message digest υπολογίζεται βάσει της χρονοσφραγίδας της υπογραφής και του τμήματος μηνύματος. Ο συνυπολογισμός της χρονοσφραγίδας της υπογραφής στο message digest προφυλάσσει από επαναληπτικές επιθέσεις. Η εξαίρεση των τμημάτων όνομα αρχείου και χρονοσφραγίδα από το τμήμα μηνύματος εξασφαλίζει ότι οι μεμονωμένες υπογραφές είναι ίδιες με τις προσαρτημένες υπογραφές που επικολλούνται στην αρχή του μηνύματος. Οι μεμονωμένες υπογραφές υπολογίζονται σε ξεχωριστό αρχείο που δεν έχει κανένα από τα βασικά πεδία του τμήματος μηνύματος.

- **key-ID του δημοσίου κλειδιού του αποστολέα**: Απαιτείται για να συγκεκριμενοποιηθεί το δημόσιο κλειδί (από τα πολλά διαφορετικά δημόσια κλειδιά που αντιστοιχούν στον αποστολέα) που πρέπει να χρησιμοποιηθεί για την αποκρυπτογράφηση του message digest.

- **Πρώτες δύο οκτάδες του message digest**: Χρησιμοποιούνται για να μπορέσει ο παραλήπτης να ελέγξει αν το δημόσιο κλειδί που χρησιμοποιήθηκε για την αποκρυπτογράφηση του message digest ήταν σωστό. Αυτό γίνεται με τη σύγκριση των δύο αυτών πρώτων (μη-κρυπτογραφημένων) οκτάδων που συμπεριλαμβάνονται στην υπογραφή με τις δύο πρώτες οκτάδες του αποκρυπτογραφημένου message digest (με το δημόσιο κλειδί που προσδιορίστηκε παραπάνω). Αυτές οι οκτάδες λειτουργούν επίσης σαν μια 16-bit ακολουθία ελέγχου για το μήνυμα.

Αξίζει να τονιστεί ότι μόνο το message digest από τα τμήματα της ψηφιακής υπογραφής είναι κρυπτογραφημένο.

Το τμήμα μηνύματος και το (προαιρετικό) τμήμα υπογραφής μπορούν να συμπιεστούν με τον αλγόριθμο ZIP και μπορούν να κρυπτογραφηθούν με το κλειδί συνόδου.

Το **τμήμα κλειδιού συνόδου** περιλαμβάνει το κλειδί συνόδου και το αναγνωριστικό του δημοσίου κλειδιού του παραλήπτη που χρησιμοποιήθηκε από τον αποστολέα για να κρυπτογραφήσει το κλειδί συνόδου.

Το όλο μπλοκ είναι συνήθως κωδικοποιημένο με Radix-64 κωδικοποίηση.

3.2.2.8 Λίστες κλειδιών

Έχουμε δει πως τα key-IDs είναι καθοριστικά στην λειτουργία του PGP και ότι δύο key-IDs ενσωματώνονται σε κάθε μήνυμα PGP που παρέχει εμπιστευτικότητα και πιστοποίηση. Αυτά τα κλειδιά απαιτείται να οργανωθούν και να αποθηκευτούν με ένα συστηματικό τρόπο για αποτελεσματική χρήση. Η μέθοδος που χρησιμοποιείται από το PGP παρέχει ένα ζεύγος από δομές δεδομένων σε κάθε κόμβο, μία δομή δεδομένων για την αποθήκευση του ιδιωτικού/δημοσίου ζεύγους κλειδιών που ανήκει στον κόμβο και μία για την αποθήκευση των δημοσίων κλειδιών των άλλων χρηστών που γνωστοποιούνται σε αυτό τον κόμβο. Αυτές οι δομές δεδομένων, αναφέρονται αντίστοιχα ως λίστα ιδιωτικών κλειδιών και λίστα δημοσίων κλειδιών.

Το Σχήμα 19 παρουσιάζει τη γενική δομή της **λίστας ιδιωτικών κλειδιών**. Μπορούμε να δούμε τη λίστα σαν ένα πίνακα στον οποίο κάθε γραμμή αναπαριστά ένα από τα ζεύγη δημοσίου/ιδιωτικού κλειδιού που κατέχει ο συγκεκριμένος χρήστης. Κάθε γραμμή περιέχει τις ακόλουθες καταχωρήσεις:

- Χρονοσφραγίδα: Η μέρα/ώρα που δημιουργήθηκε το ζεύγος κλειδιών.
- Key-ID: Τα πρώτα 64 σημαντικά bits του δημοσίου κλειδιού για αυτή την καταχώρηση.
- Δημόσιο κλειδί: Το τμήμα του δημοσίου κλειδιού του ζεύγους.
- Ιδιωτικό κλειδί: Το τμήμα του ιδιωτικού κλειδιού του ζεύγους (το πεδίο αυτό είναι κρυπτογραφημένο).
- User-ID: Συνήθως είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη (π.χ., papageorge@yahoo.gr). Ωστόσο, ο χρήστης μπορεί να προτιμήσει να συσχετίσει διαφορετικό όνομα με κάθε ζεύγος κλειδιών (π.χ., Papageorge, LPapageorge, LuisPapageorge, κ.λ.π.) ή να επαναχρησιμοποιήσει το ίδιο αναγνωριστικό κλειδιού περισσότερο από μία φορά.

Η λίστα ιδιωτικών κλειδιών μπορεί να δεικτοδοτηθεί είτε με το αναγνωριστικό χρήστη (user-ID) ή με το αναγνωριστικό κλειδιού (key-ID). (Αργότερα θα δούμε το νόημα της δυνατότητας δεικτοδότησης με δύο διαφορετικούς τρόπους.)

Αν και η λίστα ιδιωτικών κλειδιών επρόκειτο να αποθηκευτεί μόνο στη μηχανή του χρήστη που δημιουργεί και κατέχει τα ζεύγη κλειδιών, έτσι που να είναι προσπελάσιμη μόνο από αυτό το χρήστη, δεν είναι παράλογο να αποθηκευτεί το ιδιωτικό κλειδί με τον ασφαλέστερο δυνατό τρόπο. Για το λόγο αυτό δεν αποθηκεύεται το ίδιο το ιδιωτικό κλειδί στη λίστα κλειδιών, αλλά μια κρυπτογραφημένη έκδοσή του (χρησιμοποιώντας τον IDEA ή τον 3DES ή τον CAST-128). Η διαδικασία αυτή περιγράφεται παρακάτω:

1. Ο χρήστης επιλέγει μια κωδική φράση που θα χρησιμοποιηθεί για την κρυπτογράφηση των ιδιωτικών κλειδιών.

Λίστα ιδιωτικών κλειδιών				
Χρονοσφραγίδα	Key-ID*	Δημόσιο κλειδί	Κρυπτογραφημένο ιδιωτικό κλειδί	User-ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(Pi)}[KR_i]$	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

Λίστα δημοσίων κλειδιών							
Χρονοσφραγίδα	Key-ID*	Δημόσιο κλειδί	Εμπιστοσύνη κατόχου	User-ID*	Νομιμότητα κλειδιού	Υπογραφή	Εμπιστοσύνη υπογραφών
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	$KU_i \bmod 2^{64}$	KU_i	$Trust\_flag_i$	$User_i$	$Trust\_flag_i$		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

* = βασικό πεδίο για τη δεικτοδότηση του πίνακα

Σχήμα 19: Γενική δομή των λιστών ιδιωτικών και δημοσίων κλειδιών

2. Όταν το σύστημα παράγει ένα νέο ζεύγος δημοσίου/ιδιωτικού κλειδιού χρησιμοποιώντας τον RSA, ρωτάει το χρήστη για την κωδική φράση. Χρησιμοποιώντας τον SHA-1, παράγεται ένας κωδικός κατακερματισμού των 160-bits από την κωδική φράση και η κωδική φράση απορρίπτεται.

3. Το σύστημα κρυπτογραφεί το ιδιωτικό κλειδί χρησιμοποιώντας τον CAST-128 με τα 128 bits του κωδικού κατακερματισμού ως κλειδί. Τότε, ο κώδικας κατακερματισμού απορρίπτεται και το κρυπτογραφημένο ιδιωτικό κλειδί αποθηκεύεται στη λίστα ιδιωτικών κλειδιών.

Στη συνέχεια, όταν ο χρήστης προσπελαύνει τη λίστα ιδιωτικών κλειδιών για να ανακτήσει ένα ιδιωτικό κλειδί, πρέπει να παρέχει την κωδική φράση. Το PGP θα ανακτήσει το κρυπτογραφημένο ιδιωτικό κλειδί από τη λίστα, θα παράγει τον κωδικό κατακερματισμού της κωδικής φράσης και θα αποκρυπτογραφήσει το κρυπτογραφημένο ιδιωτικό κλειδί χρησιμοποιώντας τον CAST-128 με κλειδί τον κωδικό κατακερματισμού.

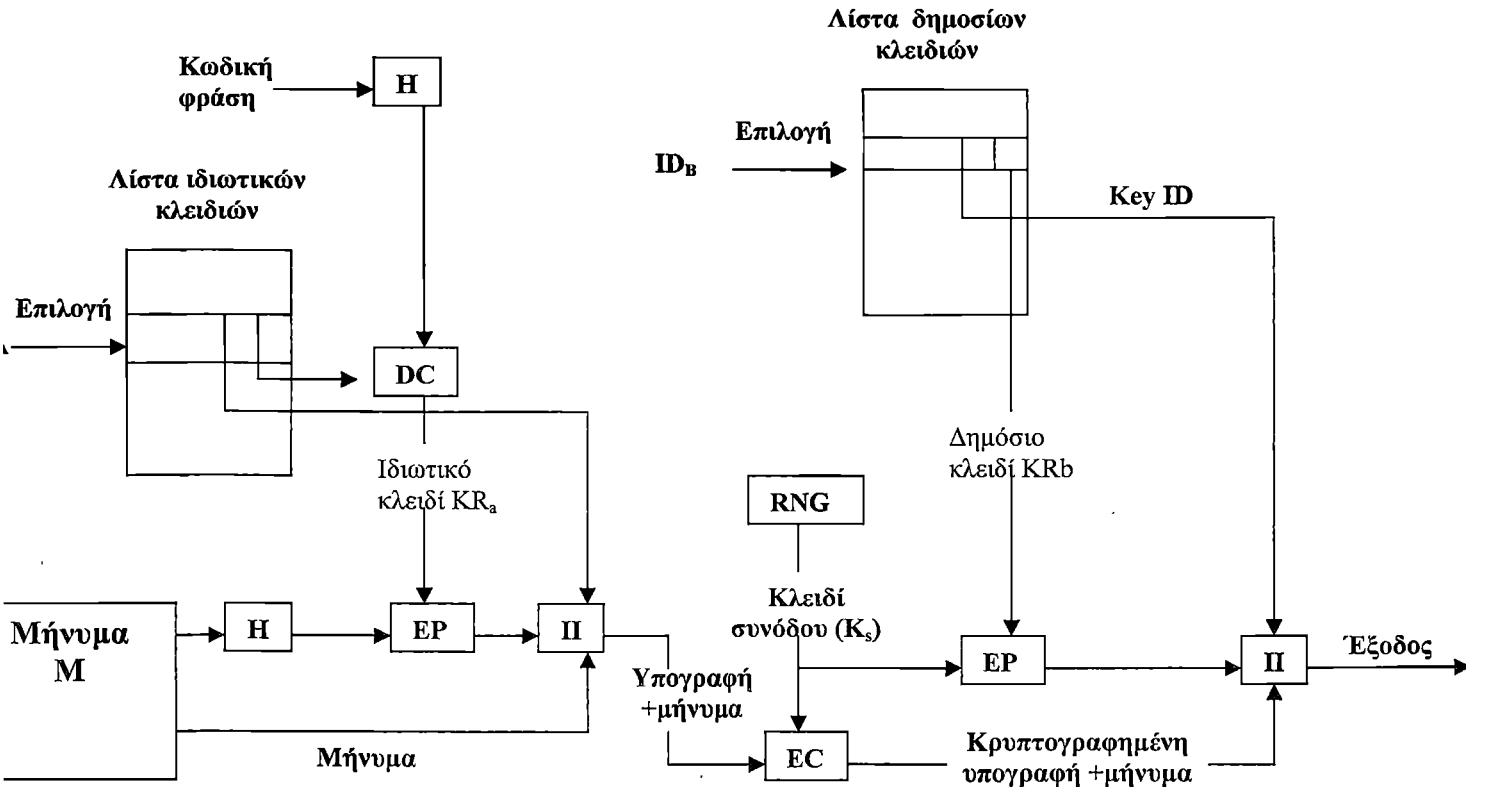
Αυτό είναι ένα περιεκτικό και αποτελεσματικό σχήμα. Όπως σε κάθε σύστημα βασισμένο σε κωδικές λέξεις, η ασφάλεια του συστήματος εξαρτάται από την ασφάλεια της κωδικής λέξης. Για να αποφύγει τον πειρασμό να τη γράψει κάπου, ο χρήστης πρέπει να χρησιμοποιήσει μια κωδική φράση που να μην είναι εύκολα προβλέψιμη, αλλά να μπορεί να τη θυμάται εύκολα.

Το Σχήμα 19 παρουσιάζει επίσης τη γενική δομή μιας **λίστας δημοσιών κλειδιών**. Αυτή η δομή δεδομένων χρησιμοποιείται για την αποθήκευση δημοσίων κλειδιών άλλων χρηστών. Για την ώρα ας αψηφήσουμε μερικά πεδία του πίνακα, περιγράφοντας μόνο τα ακόλουθα:

- Χρονοσφραγίδα: Η μέρα/ώρα που δημιουργήθηκε το ζεύγος κλειδιών.
- Key-ID: Τα πρώτα 64 σημαντικά bits του δημοσίου κλειδιού για αυτή την καταχώρηση.
- Δημόσιο κλειδί: Το δημόσιο κλειδί για αυτή την καταχώρηση.
- User-ID: Το αναγνωριστικό του κατόχου αυτού του κλειδιού. Πολλά αναγνωριστικά χρηστών μπορούν να συσχετιστούν με ένα μόνο δημόσιο κλειδί.

Η λίστα δημοσίων κλειδιών μπορεί να δεικτοδοτηθεί είτε με το αναγνωριστικό χρήστη ή με το αναγνωριστικό κλειδιού. (Αργότερα θα δούμε το νόημα της δυνατότητας δεικτοδότησης με δύο διαφορετικούς τρόπους.)

Θα περιγράψουμε τώρα πως αυτές οι λίστες κλειδιών χρησιμοποιούνται στην εκπομπή και λήψη μηνυμάτων. Για λόγους απλότητας, αψηφούμε τη συμπίεση και τη μετατροπή Radix-64 στην ακόλουθη περιγραφή. Εξετάζουμε πρώτα την εκπομπή μηνύματος. Θεωρούμε ότι το μήνυμα είναι υπογεγραμμένο και κρυπτογραφημένο.



Σχήμα 20: Παραγωγή μηνύματος PGP (από το χρήστη Α στο χρήστη Β, χωρίς συμπίεση ή μετατροπή Radix-64)

Ο αποστολέας της εφαρμογής PGP (Σχήμα 20) εκτελεί τα παρακάτω βήματα.

1. Υπογράφοντας το μήνυμα:

i. Το PGP ανακτά το κατάλληλο ιδιωτικό κλειδί από τη λίστα ιδιωτικών κλειδιών δεικτοδοτώντας την με το αναγνωριστικό χρήστη του παραλήπτη. Αν το αναγνωριστικό χρήστη του αποστολέα δεν παρέχεται στην εντολή, ανακτείται το πρώτο ιδιωτικό κλειδί στη λίστα.

ii. Το PGP απαιτεί από τον χρήστη να εισάγει την κωδική φράση ώστε να αποκρυπτογραφήσει το κρυπτογραφημένο ιδιωτικό κλειδί.

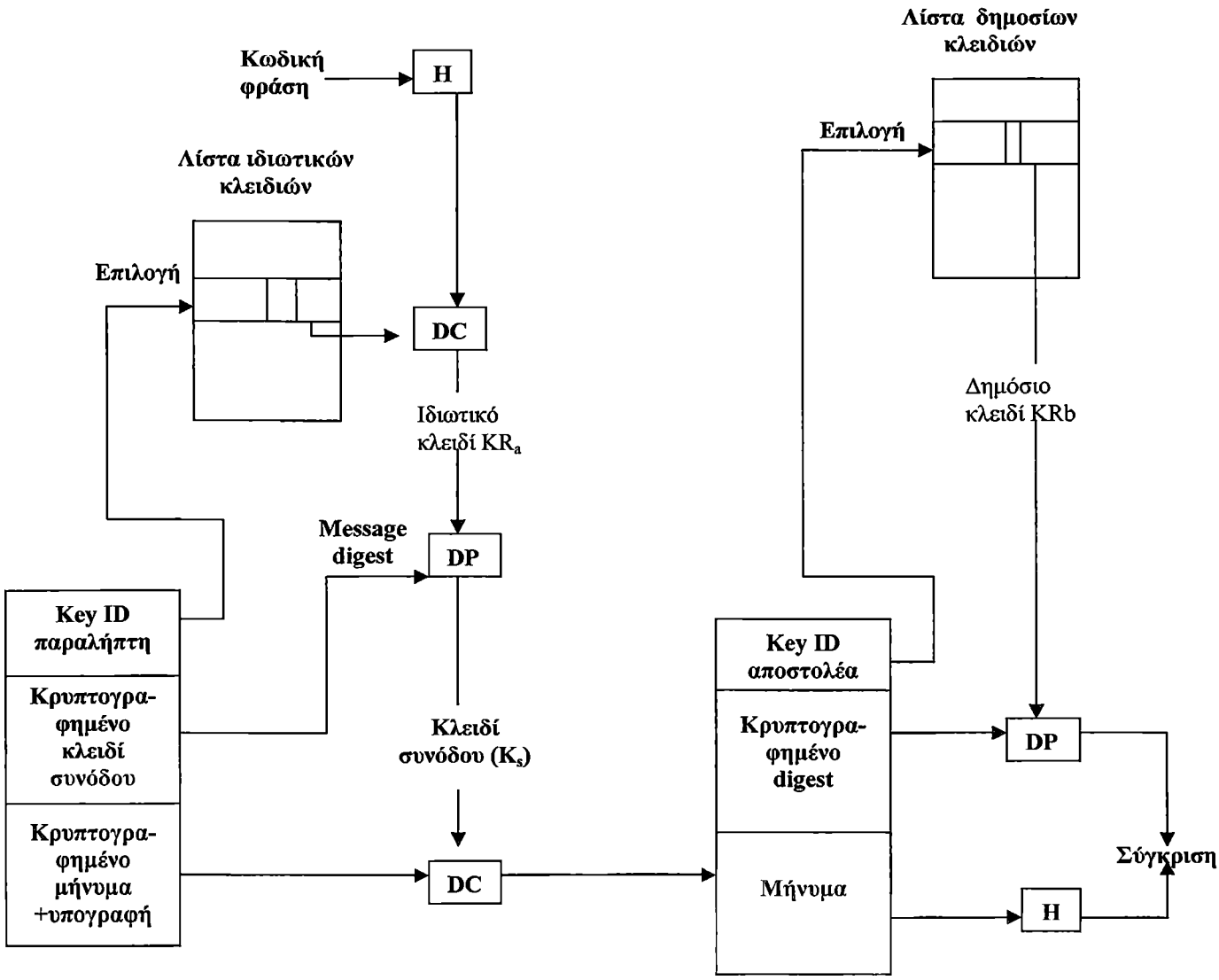
iii. Δημιουργεί το τμήμα υπογραφής του μηνύματος.

2. Κρυπτογραφώντας το μήνυμα:

i. Το PGP παράγει ένα κλειδί συνόδου και κρυπτογραφεί το μήνυμα.

ii. Το PGP ανακτά το δημόσιο κλειδί του παραλήπτη από τη λίστα δημοσίων κλειδιών δεικτοδοτώντας την με το αναγνωριστικό χρήστη του αποστολέα.

iii. Δημιουργείται το τμήμα κλειδιού συνόδου του μηνύματος.



Σχήμα 21: Λήψη μηνύματος PGP (από το χρήστη Α στο χρήστη Β, χωρίς συμπίεση ή μετατροπή Radix-64).

Ο παραλήπτης της εφαρμογής PGP (Σχήμα 21) εκτελεί τα παρακάτω βήματα.

1. Αποκρυπτογραφώντας το μήνυμα:

i. Το PGP ανακτά το ιδιωτικό κλειδί του παραλήπτη από τη λίστα ιδιωτικών κλειδιών δεικτοδοτώντας την με το αναγνωριστικό κλειδιού που περιέχεται στο τμήμα κλειδιού συνόδου του μηνύματος.

ii. Το PGP απαιτεί από το χρήστη να εισάγει την κωδική φράση ώστε να αποκρυπτογραφήσει το κρυπτογραφημένο ιδιωτικό κλειδί.

iii. Το PGP τότε ανακαλύπτει το κλειδί συνόδου και αποκρυπτογραφεί το μήνυμα.

2. Πιστοποιώντας το μήνυμα:

i. Το PGP ανακτά το δημόσιο κλειδί του αποστολέα από τη λίστα δημοσίων κλειδιών δεικτοδοτώντας την με το αναγνωριστικό κλειδιού που περιέχεται στο τμήμα υπογραφής.

ii. Το PGP ανακαλύπτει το εκπεμπόμενο message digest.

iii. Το PGP υπολογίζει το message digest για το ληφθέν μήνυμα και το συγκρίνει με το

εκπεμπόμενο message digest προς πστοποίηση.

3.2.2.9 Διαχείριση δημοσίου κλειδιού

Για ολοκλήρωση του συστήματος, το θέμα της διαχείρισης δημοσίου κλειδιού απαιτείται να εξεταστεί. Όπως αναφέρεται στα εγχειρίδια του PGP, η όλη ασχολία της προστασίας δημοσίων κλειδιών από πλαστογράφηση, είναι το πιο δύσκολο πρόβλημα στις πρακτικές εφαρμογές δημοσίου κλειδιού. Αυτό αποτελεί την "Αχίλλειο πτέρνα" της κρυπτογράφησης δημοσίου κλειδιού, και αρκετά σύνθετα λογισμικά έχουν αναπτυχθεί για την επίλυση αυτού του προβλήματος.

Το PGP παρέχει μια δομή για την επίλυση αυτού του προβλήματος (με αρκετές προτεινόμενες επιλογές που μπορούν να ακολουθηθούν).

Προσέγγιση της Διαχείρισης δημοσίου κλειδιού

Η ουσία του προβλήματος είναι η εξής: Ο χρήστης Α πρέπει να αναπτύξει μία λίστα δημοσίων κλειδιών που θα περιέχει τα δημόσια κλειδιά των άλλων χρηστών που θα αλληλογραφεί μαζί τους με τη χρήση του PGP. Ας υποθέσουμε ότι η λίστα κλειδιών του Α περιέχει ένα δημόσιο κλειδί που αποδίδεται στο χρήστη Β, αλλά το κλειδί στην πραγματικότητα κατέχεται από τον C. Αυτό θα μπορούσε να συμβεί, αν για παράδειγμα, ο Α πήρε το κλειδί από έναν ηλεκτρονικό πίνακα ενημέρωσης (BBS-Bulletin Board System) που χρησιμοποιήθηκε από τον Β για να ταχυδρομήσει το δημόσιο κλειδί, αλλά αυτό έχει προσβληθεί από τον C. Το αποτέλεσμα είναι ότι τώρα υπάρχουν δύο απειλές. Πρώτον, ο C μπορεί να στείλει μηνύματα στον Α και να πλαστογραφήσει την υπογραφή του Β, έτσι ώστε ο Α να δεχτεί το μήνυμα ως προερχόμενο από τον Β. Δεύτερον, κάθε κρυπτογραφημένο μήνυμα από τον Α στον Β μπορεί να διαβαστεί από τον C.

Ένας αριθμός από προσεγγίσεις είναι υποψήφιες για ελαχιστοποίηση του κινδύνου η λίστα δημοσίων κλειδιών ενός χρήστη να περιέχει λάθος κλειδιά. Ας υποθέσουμε ότι ο Α επιθυμεί να λάβει ένα αξιόπιστο δημόσιο κλειδί για τον Β. Οι ακόλουθες είναι κάποιες από τις προσεγγίσεις που μπορούν να χρησιμοποιηθούν:

1. **Η φυσική λήψη του κλειδιού από τον Β.** Ο Β μπορεί να αποθηκεύσει το δημόσιο κλειδί του (KU_b) σε μία δισκέτα και να το παραδώσει στον Α. Ο Α μπορεί έτσι να μεταφέρει το κλειδί στο σύστημά του μέσω της δισκέτας. Αυτή η μέθοδος είναι πολύ ασφαλής αλλά έχει προφανείς πρακτικούς περιορισμούς.

2. **Επιβεβαίωση κλειδιού μέσω τηλεφώνου.** Αν ο Α μπορεί να αναγνωρίσει τον Β στο τηλέφωνο, ο Α θα μπορούσε να καλέσει τον Β και να του ζητήσει την υπαγόρευση του κλειδιού σε μορφοποίηση Radix-64 μέσω του τηλεφώνου. Εναλλακτικά, ως μία πιο πρακτική λύση, ο Β θα μπορούσε να στείλει το κλειδί του μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στον Α. Ο Α τότε, μέσω του PGP θα μπορούσε να παράγει ένα SHA-1 digest των 160-bit του κλειδιού και να την απεικονίσει σε δεκαεξαδική μορφή. Αυτό αναφέρεται ως το "δακτυλικό αποτύπωμα" του κλειδιού. Ο Α μπορεί τότε να καλέσει τον Β και να του ζητήσει να του υπαγορεύσει το δακτυλικό αποτύπωμα μέσω τηλεφώνου. Εάν τα δύο δακτυλικά αποτυπώματα ταιριάζουν, το κλειδί επικυρώνεται.

3. **Αποκτώντας το δημόσιο κλειδί του Β από ένα αμοιβαίας εμπιστοσύνης άτομο D.** Για αυτό το σκοπό, ο χρήστης D δημιουργεί ένα υπογεγραμμένο πιστοποιητικό. Το πιστοποιητικό περιέχει το δημόσιο κλειδί του Β, το χρόνο δημιουργίας και τη χρονική περίοδο εγκυρότητας του κλειδιού. Ο D παράγει ένα SHA-1 digest του πιστοποιητικού, το κρυπτογραφεί με το ιδιωτικό κλειδί του και προσαρτεί την υπογραφή αυτή στο πιστοποιητικό. Επειδή μόνο ο D θα μπορούσε να έχει δημιουργήσει την υπογραφή, κανείς άλλος δεν μπορεί να δημιουργήσει ένα πλαστό κλειδί και να ισχυριστεί ότι αυτό έχει υπογραφεί από τον D. Η υπογεγραμμένη πιστοποίηση μπορεί να σταλεί άμεσα στον Α από τον Β ή τον D ή μπορεί να καταχωρηθεί σε πίνακα ανακοινώσεων.

4. **Αποκτώντας το δημόσιο κλειδί του Β από μια έμπιστη πιστοποιημένη αρχή.** Και στην

περίπτωση αυτή, ένα πιστοποιητικό δημοσίου κλειδιού δημιουργείται και υπογράφεται από την αρχή. Ο Α τότε θα μπορούσε να έχει πρόσβαση στην αρχή, παρέχοντας ένα όνομα χρήστη και λαμβάνοντας ένα υπογεγραμμένο πιστοποιητικό.

Για τις περιπτώσεις 3 και 4, ο Α θα έπρεπε να έχει ήδη ένα αντίγραφο από το δημόσιο κλειδί του μεσάζοντα που κάνει τη σύσταση, καθώς και την πεποίθηση ότι αυτό το κλειδί είναι έγκυρο. Σε τελευταία ανάλυση, είναι στην κρίση του Α να καθορίσει το επίπεδο εμπιστοσύνη για τον καθένα που ενεργεί ως συστήνων.

Η Χρήση Εμπιστοσύνης

Το PGP παρέχει μια κατάλληλη προσέγγιση της χρήσης εμπιστοσύνης, συνδυάζοντας την εμπιστοσύνη με δημόσια κλειδιά και αξιοποιώντας πληροφορίες εμπιστοσύνης.

Η βασική δομή είναι η ακόλουθη. Κάθε καταχώρηση στη λίστα δημοσίων κλειδιών είναι ένα πιστοποιητικό δημοσίου κλειδιού όπως προαναφέρθηκε στην προηγούμενη υποενότητα. Κάθε τέτοια καταχώρηση είναι επίσης συνδυασμένη με ένα **πεδίο γνησιότητας κλειδιών** που απεικονίζει το βαθμό εμπιστοσύνης του PGP όσον αφορά την εγκυρότητα των δημόσιων κλειδιών άλλων χρηστών. Όσο πιο υψηλό είναι το επίπεδο εμπιστοσύνης, τόσο ισχυρότερος είναι ο σύνδεσμος του αναγνωριστικού χρήστη στο κλειδί αυτό. Αυτό το πεδίο υπολογίζεται από το PGP. Επίσης, συσχετισμένες με την καταχώρηση αυτή ενδέχεται να είναι μερικές υπογραφές για το πιστοποιητικό αυτό που ο κάτοχος της λίστας κλειδιών έχει συλλέξει. Ομοίως, κάθε υπογραφή έχει συσχετιστεί με ένα **πεδίο εμπιστοσύνης υπογραφών** που απεικονίζει το βαθμό στον οποίο ο χρήστης PGP εμπιστεύεται τον υπογράφων που πιστοποιεί τα δημόσια κλειδιά. Το πεδίο γνησιότητας κλειδιών απορρέει από τη συλλογή των πεδίων εμπιστοσύνης υπογραφών της καταχώρησης. Τέλος, κάθε καταχώρηση καθορίζει ένα δημόσιο κλειδί που συσχετίζεται με ένα συγκεκριμένο νόμιμο κάτοχο και περιέχει ένα **πεδίο εμπιστοσύνης νόμιμου κατόχου** το οποίο απεικονίζει το βαθμό στον οποίο αυτό το δημόσιο κλειδί είναι αξιόπιστο για να υποδείξει άλλα πιστοποιητικά δημοσίων κλειδιών. Αυτό το επίπεδο εμπιστοσύνης εκχωρείται από το χρήστη.

Τα τρία πεδία που μνημονεύτηκαν στην προηγούμενη παράγραφο απαρτίζουν μια ενιαία δομή που αποδίδεται ως trust flag byte (byte σημαίας εμπιστοσύνης). Τα περιεχόμενα αυτής της σημαίας εμπιστοσύνης για τις τρεις χρήσεις εμπιστοσύνης που αναφέρθηκαν απεικονίζονται στο Σχήμα 22.

(α) Εμπιστοσύνη εκχωρούμενη στο δημόσιο κλειδί του νόμιμου κατόχου (εμφανίζεται μετά το πακέτο κλειδιού και καθορίζεται από τον χρήστη)	(β) Εμπιστοσύνη εκχωρούμενη στο ζεύγος δημόσιο κλειδί - αναγνωριστικό χρήστη (εμφανίζεται μετά το πακέτο αναγνωριστικού χρήστη και υπολογίζεται από το PGP)	(γ) Εμπιστοσύνη εκχωρούμενη στην υπογραφή (εμφανίζεται μετά το πακέτο υπογραφής και είναι αντίγραφο της OWNERTRUST για τον υπογράφοντα)
Πεδίο OWNERTRUST • απροσδιόριστη εμπιστοσύνη • άγνωστος χρήστης • συνήθως μη-έμπιστος να υπογράψει άλλα κλειδιά • συνήθως έμπιστος να υπογράψει άλλα κλειδιά • αυτό το κλειδί παρουσιάζεται στη λίστα μυστικών κλειδιών (απόλυτη εμπιστοσύνη) **BUCKSTOP bit** • είναι 1 αν αυτό το κλειδί εμφανίζεται στη λίστα μυστικών κλειδιών	**Πεδίο KEYLEGIT** • άγνωστη ή απροσδιόριστη εμπιστοσύνη • κυριότητα κλειδιού μη έμπιστη • οριακή εμπιστοσύνη στην κυριότητα κλειδιού • πλήρης εμπιστοσύνη στην κυριότητα κλειδιού **WARNONLY bit** • είναι 1 αν ο χρήστης επιθυμεί να ειδοποιηθεί μόνο όταν ένα κλειδί που δεν είναι πλήρως επικυρωμένο χρησιμοποιείται για κρυπτογράφηση	**Πεδίο SIGTRUST** • απροσδιόριστη εμπιστοσύνη • άγνωστος χρήστης • συνήθως μη-έμπιστος να υπογράψει άλλα κλειδιά • συνήθως έμπιστος να υπογράψει άλλα κλειδιά • πάντα έμπιστος να υπογράψει άλλα κλειδιά • αυτό το κλειδί παρουσιάζεται στην λίστα μυστικών κλειδιών (απόλυτη εμπιστοσύνη) **CONTIG bit** • είναι 1 αν η υπογραφή κατευθύνει ένα συνέχομενο έμπιστο μονοπάτι πιστοποιητικού στη λίστα απόλυτης εμπιστοσύνης κλειδιών του νόμιμου κατόχου

Σχήμα 22: Περιεχόμενα του byte σημαίας εμπιστοσύνης

Ας επικεντρωθούμε στη διαχείριση της λίστας δημοσίων κλειδιών του χρήστη Α. Η διαδικασία εμπιστοσύνης είναι η ακόλουθη:

1. Όταν ο Α εισάγει ένα νέο δημόσιο κλειδί στη λίστα του δημοσίων κλειδιών, το PGP πρέπει να καταχωρήσει μία τιμή στη σημαία εμπιστοσύνης που συσχετίζεται με το νόμιμο κάτοχο αυτού του κλειδιού. Αν ο κάτοχος είναι ο Α και επομένως αυτό το δημόσιο κλειδί εμφανίζεται στη λίστα ιδιωτικών κλειδιών του, η τιμή απόλυτης εμπιστοσύνης εκχωρείται αυτόματα στο πεδίο εμπιστοσύνης. Διαφορετικά, το PGP ρωτάει τον Α για την εκτίμησή του σχετικά με την εμπιστοσύνη που θα πρέπει να εκχωρήσει στον κάτοχο αυτού του κλειδιού. Ο Α θα πρέπει τότε να εισάγει το επιθυμητό επίπεδο. Ο χρήστης μπορεί να προσδιορίσει ότι ο κάτοχος του είναι άγνωστος, μη έμπιστος, οριακής εμπιστοσύνης ή απόλυτης εμπιστοσύνης.

2. Όταν εισάγεται ένα νέο δημόσιο κλειδί, μία ή περισσότερες υπογραφές μπορούν να προσαρτηθούν σε αυτό, ενώ επιπλέον υπογραφές μπορούν να προστεθούν αργότερα. Όταν μια υπογραφή εισάγεται στην καταχώρηση, το PGP εξετάζει τη λίστα δημοσίων κλειδιών για να βρει αν ο εκδότης της υπογραφής υπάρχει μεταξύ των νόμιμων κατόχων δημοσίων κλειδιών. Αν όντως υπάρχει, η τιμή OWNERTRUST για τον κάτοχο εκχωρείται στο πεδίο SIGTRUST για την υπογραφή. Διαφορετικά, η τιμή "άγνωστος χρήστης" εκχωρείται.

3. Η τιμή του πεδίου γνησιότητας κλειδιού υπολογίζεται στη βάση του πεδίου εμπιστοσύνης υπογραφών που παρουσιάζεται σε αυτή την καταχώρηση. Αν μία τουλάχιστον υπογραφή έχει την τιμή εμπιστοσύνης υπογραφής "απόλυτη", τότε η τιμή γνησιότητας κλειδιού γίνεται "πλήρης". Διαφορετικά το PGP υπολογίζει ένα άθροισμα από τιμές εμπιστοσύνης με συντελεστές βαρύτητας. Σε υπογραφές που είναι πάντα αξιόπιστες αποδίδεται βάρος 1/Χ,

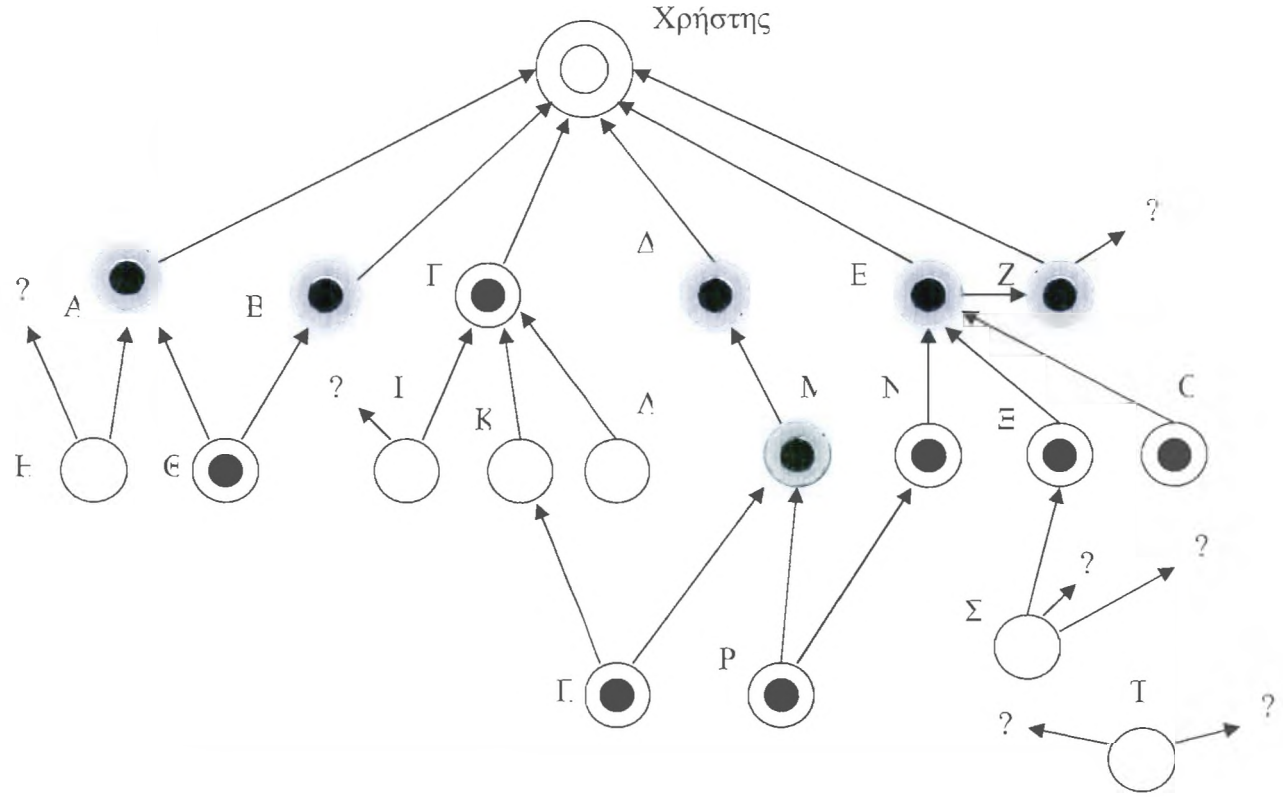
ενώ σε υπογραφές που είναι συνήθως αξιόπιστες αποδίδεται βάρος 1/Υ, όπου Χ και Υ είναι παράμετροι που διαμορφώνονται από το χρήστη. Όταν το άθροισμα των βαρών ενός συνδυασμού κλειδιού/αναγνωριστή χρήστη (που παρέχονται από τους χρήστες που συστήνουν τον συνδυασμό αυτό) γίνει 1, τότε η σύνδεση είναι αξιόπιστη και η γνησιότητα κλειδιού παίρνει την τιμή "πλήρης". Έτσι, στην περίπτωση απουσίας απόλυτης εμπιστοσύνης, απαιτούνται είτε τουλάχιστον Χ υπογραφές που είναι πάντα έμπιστες ή τουλάχιστον Υ υπογραφές που είναι συνήθως αξιόπιστες ή κάποιος συνδυασμός τους.

Περιοδικά, το PGP επεξεργάζεται τη λίστα δημοσίων κλειδιών για να διατηρήσει τη συνέπεια. Αυτή είναι μία διαδικασία αναζήτησης κατά βάθος. Για κάθε πεδίο OWNERTRUST, το PGP σαρώνει τη λίστα για να βρει τις υπογραφές που εκδόθηκαν από τον ίδιο νόμιμο κάτοχο και ενημερώνει το πεδίο SIGTRUST έτσι ώστε να ισούται με το πεδίο OWNERTRUST. Αυτή η διαδικασία ξεκινά από τα κλειδιά στα οποία υπάρχει απόλυτη εμπιστοσύνη. Τότε όλα τα πεδία KEYLEGIT υπολογίζονται με βάση τις προσαρτημένες υπογραφές.

Το Σχήμα 23 δίνει ένα παράδειγμα του τρόπου συσχέτισης της αξιοπιστίας της υπογραφής με τη γνησιότητα του κλειδιού. Το σχήμα αποτελεί μια απεικόνιση της δομής λίστας δημοσίων κλειδιών. Ο χρήστης έχει αποκτήσει έναν αριθμό από δημόσια κλειδιά, κάποια άμεσα από τους νόμιμους κατόχους τους και κάποια έμμεσα από κάποιον εξυπηρέτη κλειδιών.

Ο κόμβος με την περιγραφή "Χρήστης" αναφέρεται στην καταχώρηση της λίστας δημοσίων κλειδιών που αντιστοιχεί σε αυτό τον χρήστη. Αυτό το κλειδί είναι γνήσιο και η τιμή OWNERTRUST είναι "απόλυτης εμπιστοσύνης". Κάθε άλλος κόμβος στη λίστα κλειδιών έχει απροσδιόριστη τιμή στο πεδίο OWNERTRUST, εκτός και αν κάποια άλλη τιμή έχει καταχωρηθεί από το χρήστη. Σε αυτό το παράδειγμα, ο χρήστης έχει καθορίσει ότι πάντα εμπιστεύεται τους χρήστες Δ, Ε, Ζ και Μ για να υπογράφουν άλλα κλειδιά. Επίσης, για το σκοπό αυτό, ο χρήστης εμπιστεύεται μερικώς τους χρήστες Α και Β.

Άρα η σκίαση και η έλλειψη σκίασης γύρω από τον κόμβο στο Σχήμα 23 απεικονίζει το επίπεδο εμπιστοσύνης που καταχωρείται από το χρήστη. Η δομή δέντρου δείχνει ποια κλειδιά και από ποιούς άλλους χρήστες έχουν υπογραφεί. Αν ένα κλειδί έχει υπογραφεί από ένα χρήστη του οποίου το κλειδί είναι επίσης στη λίστα κλειδιών, ένα βέλος συνδέει το υπογεγραμμένο κλειδί με τον υπογράφοντα. Αν το κλειδί έχει υπογραφεί από ένα χρήστη του οποίου το κλειδί δεν παρουσιάζεται σε αυτή τη λίστα κλειδιών, το βέλος συνδέει το υπογεγραμμένο κλειδί με ένα ερωτηματικό, υποδεικνύοντας ότι ο υπογράφων είναι άγνωστος σε αυτό το χρήστη.



? = άγνωστος υπογράφων

X → Y = ο Χ έχει υπογραφεί από τον Υ

= το κλειδί του νόμιμου κατόχου είναι αξιόπιστο από εμάς για να υπογράφει κλειδιά

= το κλειδί του νόμιμου κατόχου είναι μερικώς αξιόπιστο από εμάς για να υπογράφει κλειδιά

= το κλειδί έχει κριθεί ως γνήσιο από εμάς

Σχήμα 23: Παράδειγμα μοντέλου εμπιστοσύνης του PGP

Το Σχήμα 23 αναδεικνύει αρκετά σημεία που μπορούν να γίνουν παρατηρήσεις:

1. Όλα τα κλειδιά των οποίων οι νόμιμοι κάτοχοι είναι πλήρως ή μερικώς έμπιστοι στο χρήστη έχουν υπογραφεί από τον ίδιο το χρήστη με εξαίρεση τον κόμβο Μ. Όπως δείχνει ο κόμβος Μ, η υπογραφή ενός χρήστη δεν είναι πάντα υποχρεωτική, αλλά στην πράξη, οι περισσότεροι χρήστες προτιμούν να υπογράφουν τα κλειδιά για τους περισσότερους κατόχους που εμπιστεύονται. Έτσι, για παράδειγμα παρά το ότι το κλειδί του Ε έχει ήδη υπογραφεί από έμπιστο μεσάζοντα, τον Ζ, ο χρήστης διαλέγει να υπογράψει το κλειδί του Ε άμεσα.

2. Κάνουμε την παραδοχή ότι δύο μερικώς αξιόπιστες υπογραφές είναι κατάλληλες για να πιστοποιήσουν ένα κλειδί. Συνεπώς, το κλειδί για το χρήστη Θ θεωρείται γνήσιο από το PGP διότι είναι υπογεγραμμένο από τους Α και Β οι οποίοι είναι μερικώς αξιόπιστοι.

3. Η γνησιότητα ενός κλειδιού μπορεί να επιβεβαιωθεί όταν υπογράφεται από έναν πλήρης ή από δύο μερικής εμπιστοσύνης υπογράφοντες, αλλά ο χρήστης τους μπορεί να μην θεωρείται

έμπιστος να υπογράψει άλλα κλειδιά. Για παράδειγμα, το κλειδί του Ξ είναι γνήσιο επειδή είναι υπογεγραμμένο από τον Ε τον οποίο ο χρήστης εμπιστεύεται, αλλά ο Ξ δεν θεωρείται έμπιστος να υπογράψει άλλα κλειδιά επειδή ο χρήστης δεν έχει αποδώσει στον Ξ τέτοια τιμή εμπιστοσύνης. Για το λόγο αυτό, αν και το κλειδί του Σ έχει υπογραφεί από τον Ξ, το PGP δεν θεωρεί το κλειδί του Σ γνήσιο. Η κατάσταση αυτή είναι δικαιολογημένη για τον εξής λόγο. Το ότι ο χρήστης επιθυμεί να στείλει ένα ιδιωτικό μήνυμα σε κάποιον, δεν σημαίνει απαραίτητα ότι τον εμπιστεύεται με κάθε έννοια. Είναι μόνο απαραίτητο, ο χρήστης να είναι σίγουρος ότι έχει το σωστό δημόσιο κλειδί για τον παραλήπτη.

4. Το Σχήμα 23 δείχνει επίσης ένα παράδειγμα ενός "ορφανού" κόμβου Τ με δύο άγνωστες υπογραφές. Συνήθως ένα τέτοιο κλειδί συλλέγεται από έναν εξυπηρέτη κλειδιών. Το PGP δεν μπορεί να θεωρήσει ότι ένα τέτοιο κλειδί είναι γνήσιο, απλά επειδή προέρχεται από έναν δημοσίας φήμης εξυπηρέτη. Ο χρήστης πρέπει να δηλώσει την γνησιότητα του κλειδιού υπογράφοντάς το, ή λέγοντας στο PGP ότι προτίθεται να εμπιστευθεί πλήρως έναν από τους υπογράφοντες το κλειδί.

Καταλήγουμε με μια τελική παρατήρηση. Αναφέρθηκε προηγουμένως ότι πολλά αναγνωριστικά χρηστών ενδέχεται να συσχετιστούν με ένα δημόσιο κλειδί της λίστας δημοσίων κλειδιών. Αυτό θα μπορούσε να συμβεί επειδή ένα άτομο έχει αλλάξει ονόματα ή έχει συστηθεί μέσω υπογραφών με περισσότερα ονόματα, υποδεικνύοντας για παράδειγμα διαφορετικές διευθύνσεις ηλεκτρονικού ταχυδρομείου. Έτσι μπορούμε να θεωρήσουμε ένα δημόσιο κλειδί σαν τη ρίζα ενός δέντρου. Ένα δημόσιο κλειδί έχει έναν αριθμό από αναγνωριστικά χρήστη συσχετισμένα με αυτό μαζί με έναν αριθμό υπογραφών κάτω από κάθε αναγνωριστικό χρήστη. Η σύνδεση ενός συγκεκριμένου αναγνωριστικού χρήστη με το κλειδί εξαρτάται από τις υπογραφές που σχετίζονται με αυτό το αναγνωριστικό χρήστη και το κλειδί, ενώ το επίπεδο εμπιστοσύνης αυτού του κλειδιού (για χρήση προς υπογραφή άλλων κλειδιών) είναι συνάρτηση όλων των εξαρτημένων υπογραφών.

Ανακαλώντας Δημόσια Κλειδιά

Ένας χρήστης ενδέχεται να επιθυμεί να ανακαλέσει το τρέχον δημόσιο κλειδί του είτε επειδή υποψιάζεται διακύβευση ή απλά για να αποφύγει τη χρήση του ίδιου κλειδιού για μια παρατεταμένη περίοδο. Σημειώνουμε ότι η διακύβευση μπορεί να συμβεί μόνο αν κάποιος έχει καταφέρει να αποκτήσει ένα αντίγραφο του μη κρυπτογραφημένου ιδιωτικού κλειδιού του ή αν έχει λάβει και το κρυπτογραφημένο ιδιωτικό κλειδί από τη λίστα ιδιωτικών κλειδιών και την κωδική φράση.

Για την ανάκληση ενός δημοσίου κλειδιού, ο κάτοχος πρέπει να εκδόσει ένα πιστοποιητικό ανάκλησης κλειδιών που φέρει την υπογραφή του. Αυτό το πιστοποιητικό έχει τον ίδιο τύπο με το κλασικό πιστοποιητικό υπογραφής, αλλά επιπλέον περιέχει έναν ενδείκτη που δηλώνει ότι ο σκοπός αυτού του πιστοποιητικού είναι η ανάκληση της χρήσης του δημοσίου κλειδιού. Είναι σημαντικό να σημειωθεί ότι το αντίστοιχο ιδιωτικό κλειδί πρέπει να χρησιμοποιηθεί για την υπογραφή του πιστοποιητικού ανάκλησης του δημοσίου κλειδιού. Ο νόμιμος κάτοχος πρέπει να προσπαθήσει να διαδώσει το πιστοποιητικό αυτό όσο πιο εκτεταμένα και γρήγορα γίνεται προκειμένου να ειδοποιηθούν οι ενδεχόμενοι ανταποκριτές και να ενημερώσουν τις λίστες των δημοσίων κλειδιών τους.

Σημειώνουμε ότι κάποιος εισβολέας ο οποίος έχει διακυβευτεί το ιδιωτικό κλειδί ενός νόμιμου κατόχου μπορεί επίσης να εκδόσει ένα τέτοιο πιστοποιητικό. Ωστόσο αυτό θα είχε σαν αποτέλεσμα να μην μπορεί πλέον το κλειδί να χρησιμοποιηθεί ούτε από τον εισβολέα, ούτε και από το γνήσιο κάτοχο του δημοσίου κλειδιού, και επομένως δεν θεωρείται πολύ πιθανό να συμβεί ανάκληση κλειδιού από κάποιο τέτοιο εισβολέα.

4 ΠΕΡΙΒΑΛΛΟΝ ΕΡΓΑΣΊΑΣ ΤΟΥ PGP

Πλήρες εγχειρίδιο χρήσης του PGP παρέχεται στην [PGP02-2]. Μέρος του εγχειριδίου που περιέχει τις σημαντικότερες λειτουργίες του PGP με έμφαση στις εφαρμογές ηλεκτρονικού ταχυδρομείου παρουσιάζεται στη συνέχεια.

Υπάρχουν πολλοί τρόποι να προσπελάσουμε τις λειτουργίες του PGP. Αυτό το κεφάλαιο δείχνει και περιγράφει τρόπους να προσπελάσουμε το PGP και τα βασικά μενού του:

- Κλειδιά PGP,
- Ταχυδρομείο PGP,
- Δίσκο εγγραφής PGP.

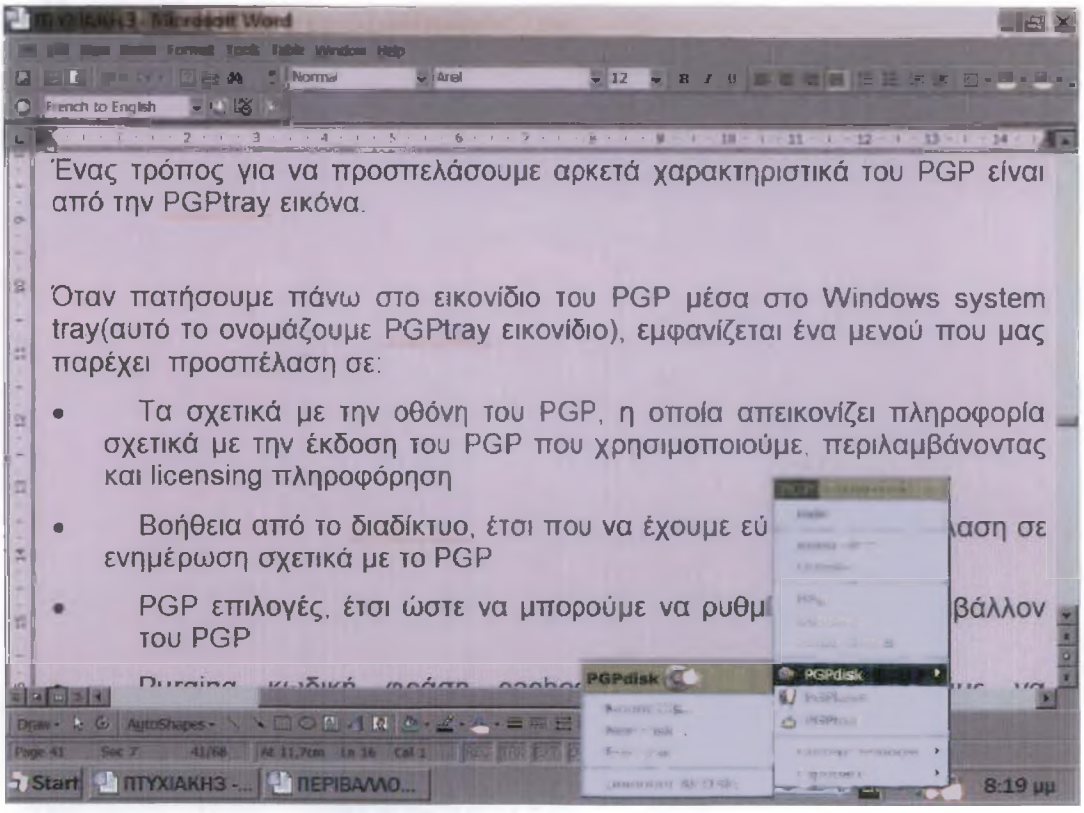
4.1 Προσπελαύνοντας το PGP

Υπάρχουν τέσσερις κύριοι τρόποι να προσπελάσουμε το PGP:

1. μέσω της PGPtray εικόνας,
2. μέσω του μενού εκκίνησης,
3. μέσω του εξερευνητή των Windows,
4. διαμέσου κάποιων εφαρμογών ηλεκτρονικού ταχυδρομείου.

4.1.1 Η PGPtray εικόνα

Ένας άμεσος τρόπος για να προσπελάσουμε αρκετά χαρακτηριστικά του PGP, είναι από το εικονίδιο PGPtray που φαίνεται στο Σχήμα 24.



Σχήμα 24: Το εικονίδιο του PGPtray.

Όταν πατήσουμε πάνω στο εικονίδιο του PGP μέσα στο Windows system tray (το οποίο ονομάζουμε εικονίδιο PGPtray) εμφανίζεται ένα μενού που μας παρέχει προσπέλαση στα ακόλουθα:

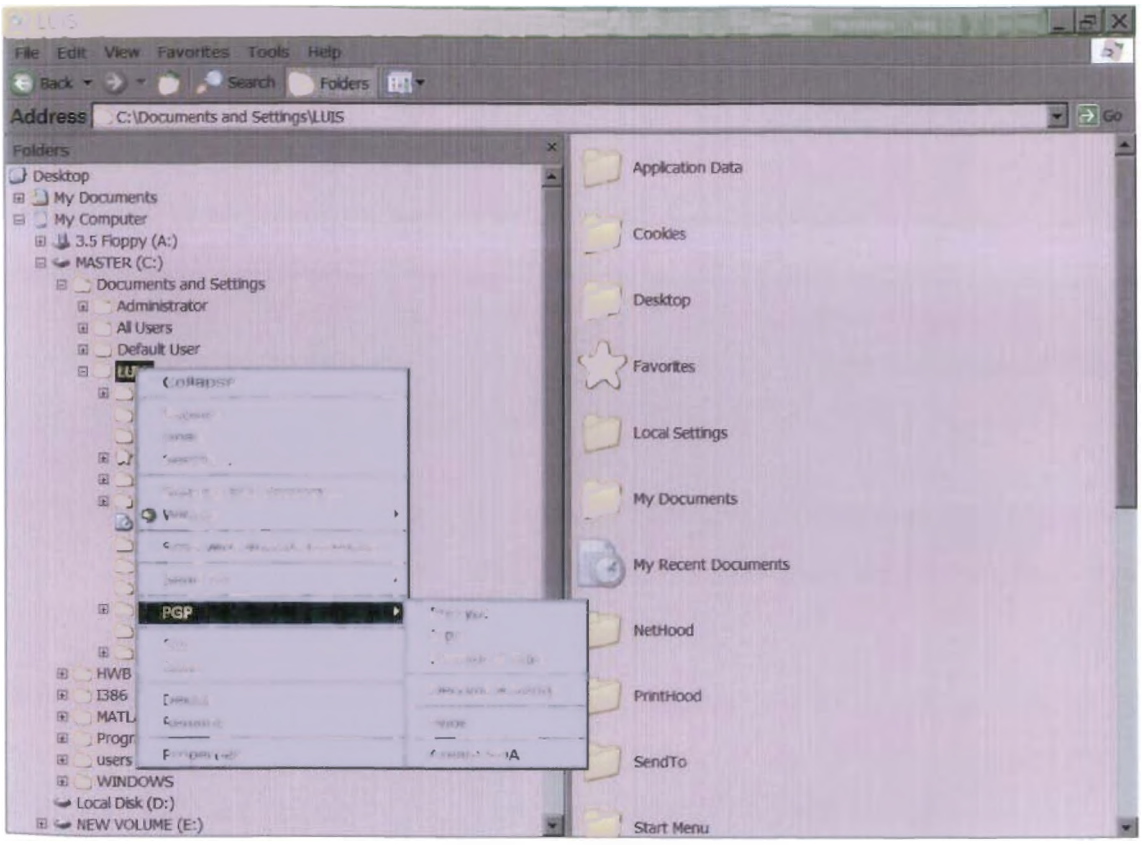
- Την οθόνη Σχετικά με το PGP (About PGP), η οποία απεικονίζει πληροφορίες σχετικά με την χρησιμοποιούμενη έκδοση του PGP και τα δικαιώματα χρήσης.
- Άμεση Βοήθεια (PGP Online Help), ώστε να έχουμε εύκολη πρόσβαση σε χρήσιμες πληροφορίες σχετικά με το PGP.
- PGP επιλογές (PGP Options), ώστε να μπορούμε να προσαρμόσουμε το περιβάλλον του PGP όπως μας ταιριάζει.
- Εκκαθάριση μνήμης κωδικών φράσεων (Purge caches), ώστε να μπορούμε να αφαιρέσουμε αποθηκευμένες κωδικές φράσεις από τη μνήμη για να αποτρέψουμε μη εξουσιοδοτημένη χρήση του PGP.
- Λειτουργίες δίσκου του PGP (PGPdisk), ώστε να έχουμε γρήγορη προσπέλαση στην λειτουργικότητα του δίσκου του PGP.
- Οι οθόνες Κλειδιών του PGP (PGPkeys) και Ηλεκτρονικού Ταχυδρομείου PGP (PGPmail), ώστε να έχουμε εύκολη πρόσβαση στη λειτουργικότητα των κλειδιών του PGP και στο ηλεκτρονικό ταχυδρομείο του PGP.
- Επιλογές κρυπτογράφησης, αποκρυπτογράφησης/επικύρωσης και υπογραφής (Current Window → Encrypt, Decrypt/Verify, Sign) για δεδομένα στο τρέχον παράθυρο, ώστε να μπορούμε να χρησιμοποιούμε με άμεσο τρόπο τη λειτουργικότητα του PGP στο τρέχον παράθυρο.
- Επιλογές εκκαθάρισης, εγγραφής, κρυπτογράφησης, αποκρυπτογράφησης/επικύρωσης και υπογραφής (Clipboard → Empty, Edit, Encrypt, Decrypt/Verify, Sign) για δεδομένα του Clipboard, ώστε να μπορούμε να χρησιμοποιούμε με άμεσο τρόπο τη λειτουργικότητα του PGP στα δεδομένα του Clipboard.

4.1.2 Εξερευνητής των Windows

Μπορούμε επίσης να προσπελάσουμε τις λειτουργίες του PGP από τον εξερευνητή των Windows, ανοίγοντας απλά τον εξερευνητή και επιλέγοντας τα αντικείμενα πάνω στα οποία θέλουμε να δουλέψουμε. Η διαδικασία αυτή περιγράφεται στο Σχήμα 25.

Ο εξερευνητής των Windows μας παρέχει προσπέλαση σε διαφορετικές λειτουργίες του PGP:

- Οδηγός (Drive): Αν επιλέξουμε με δεξί κλικ έναν οδηγό του σύστηματός μας (π.χ., A:\, B:\ , C:\, κλπ.) στον εξερευνητή των Windows και επιλέξουμε PGP από το μενού που εμφανίζεται, μπορούμε να εκτελέσουμε τις ακόλουθες λειτουργίες στον οδηγό:
  - Κρυπτογράφηση, υπογραφή, ή κρυπτογράφηση και υπογραφή των δεδομένων του.
  - Αποκρυπτογράφηση και επικύρωση των δεδομένων του.
  - Εκκαθάριση του ελεύθερου χώρου του.
  - Δημιουργία ενός αυτο-αποκρυπτογραφόμενου τόμου (Self-Decrypting Archieve, SDA) του οδηγού.



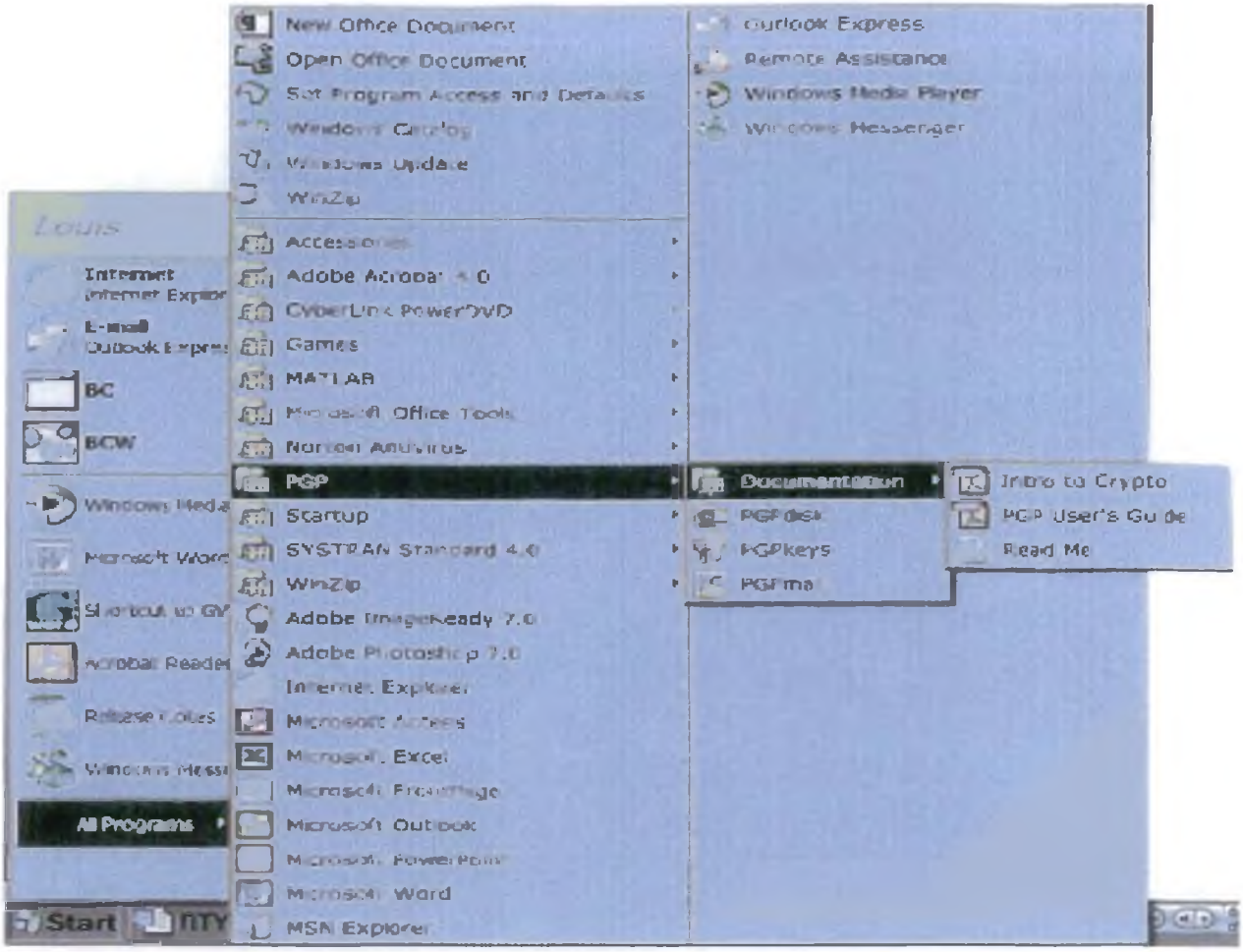
Σχήμα 25: Προσπέλαση του PGP μέσω του εξερευνητή των Windows.

- Φάκελος (Folder): Αν επιλέξουμε με δεξί κλικ έναν φάκελο στον εξερευνητή των Windows και επιλέξουμε PGP από το μενού που εμφανίζεται, μπορούμε να εκτελέσουμε τις ακόλουθες λειτουργίες στο φάκελο:
  - Κρυπτογράφηση, υπογραφή, ή κρυπτογράφηση και υπογραφή των δεδομένων του.
  - Αποκρυπτογράφηση και επικύρωσή των δεδομένων του.
  - Εκκαθάριση.
  - Δημιουργία ενός αυτό-αποκρυπτογραφόμενου τόμου (SDA) με τα περιεχόμενα του φακέλου.
- Αρχείο (File): Αν επιλέξουμε με δεξί κλικ ένα αρχείο στον εξερευνητή των Windows, το υπομενού του PGP μας επιτρέπει να επιλέξουμε μια ποικιλία από λειτουργίες πάνω στο αρχείο, που εξαρτώνται από το είδος του αρχείου:
  - Αν επιλέξουμε ένα *μη κρυπτογραφημένο αρχείο*, μπορούμε να το κρυπτογραφήσουμε, να το υπογράψουμε, να το σβήσουμε, ή να δημιουργήσουμε ένα SDA.
  - Αν επιλέξουμε ένα *κρυπτογραφημένο αρχείο*, μπορούμε να το αποκρυπτογραφήσουμε και επικυρώσουμε, ή να το σβήσουμε.
  - Αν επιλέξουμε ένα *αρχείο PGP δίσκου (.pgd)*, μπορούμε να το προσαρτήσουμε ή να το διασκευάσουμε.
  - Αν επιλέξουμε ένα *αρχείο ASCII κλειδιών (.asc)*, μπορούμε να το αποκρυπτογραφήσουμε/επικυρώσουμε, ή να το σβήσουμε. Αν επιλέξουμε αποκρυπτογράφηση/επικύρωση, παρέχεται η επιλογή εισαγωγής του αρχείου στο PGP.
  - Αν επιλέξουμε ένα αρχείο *λίστας δημοσίων ή ιδιωτικών κλειδιών* PGP (.pkr ή .skr, αντίστοιχα), μπορούμε να προσθέσουμε τα κλειδιά στην προσωπική μας λίστα

κλειδιών ή να σβήσουμε το αρχείο.

4.1.3 Το Μενού Εκκίνησης

Ένας ακόμα τρόπος προσπέλασης του PGP είναι μέσω του μενού εκκίνησης των Windows. Επιλέγουμε **Εκκίνηση**, κυλίουμε πάνω στα **Προγράμματα** και από εκει στο **PGP.**



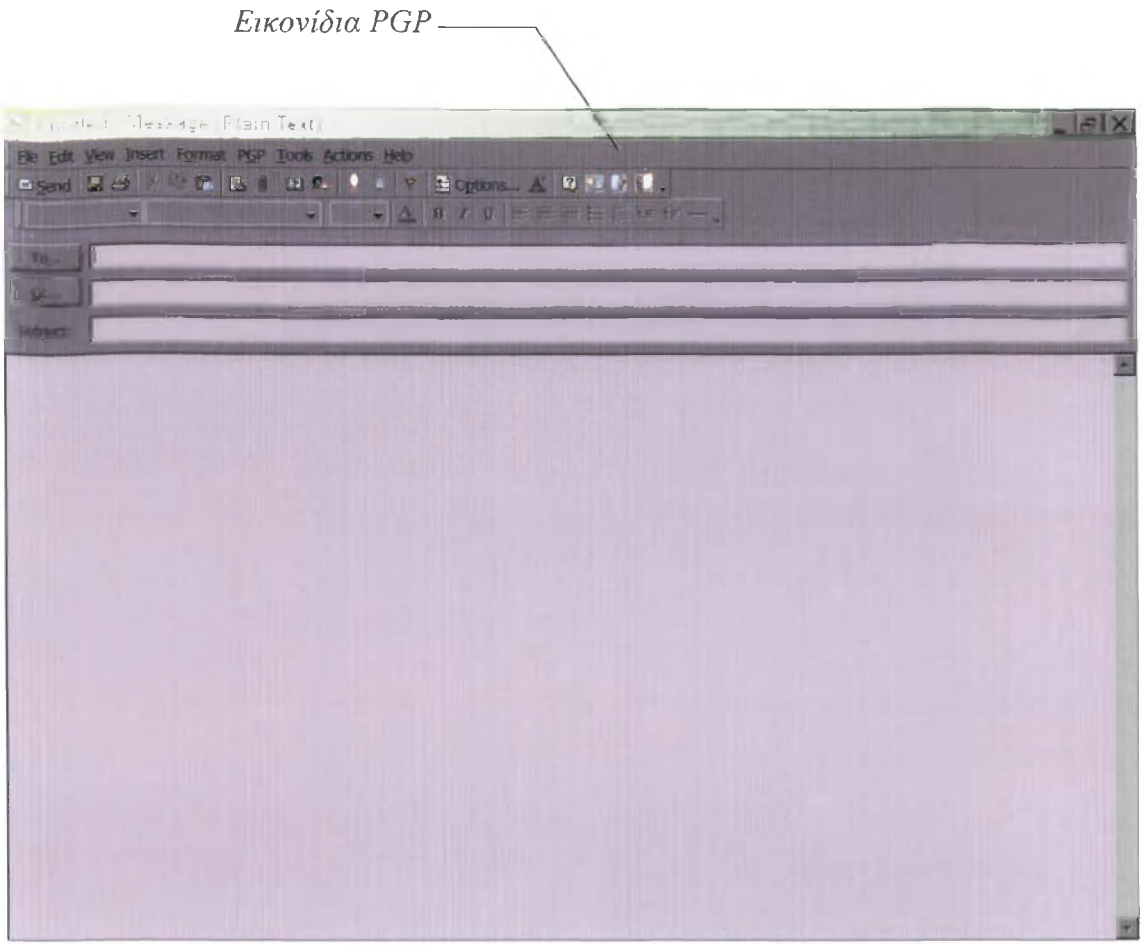
Σχήμα 26: Προσπέλαση του PGP μέσω του μενού εκκίνησης.

Το μενού Εκκίνησης επιτρέπει προσπέλαση στα ακόλουθα:

- Τεκμηρίωση PGP.
- Λειτουργίες δίσκου PGP.
- Κλειδιά του PGP και οθόνες ηλεκτρονικού ταχυδρομείου του PGP.

4.1.4 Εφαρμογές Ηλεκτρονικού Ταχυδρομείου

Μπορούμε να προσπελάσουμε μερικές λειτουργίες του PGP μέσα από συγκεκριμένες εφαρμογές ηλεκτρονικού ταχυδρομείου, όπως, π.χ., το Microsoft Outlook



Σχήμα 27: Πρόσπελαση του PGP μέσω του Microsoft Outlook

Αν έχουμε δημιουργήσει ένα νέο μήνυμα στο Outlook, η καθορισμένη μπάρα εργαλείων παρέχει εικονίδια που μας επιτρέπουν:

- Κρυπτογράφηση του μηνύματος.
- Υπογραφή του μηνύματος.
- Άνοιγμα κλειδιών PGP.

Το Outlook επίσης έχει εικονίδια του PGP για:

- Αποκρυπτογράφηση ενός μηνύματος και επικύρωση της υπογραφής του.
- Άνοιγμα κλειδιών PGP.

Το PGP εγκαθιστά εικονίδια του στις ακόλουθες εφαρμογές ηλεκτρονικού ταχυδρομείου:

- Microsoft exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes
- Novel Group Wise
- QUALCOMM Eudora

Σημείωση: Αν χρησιμοποιούμε μια εφαρμογή ηλεκτρονικού ταχυδρομείου που δεν έχει εικονίδια του PGP στη γραμμή εργαλείων της, τότε μπορούμε να χρησιμοποιήσουμε το PGPtray για να αποκτήσουμε πρόσβαση στις λειτουργίες του PGP σε κάθε τρέχον παράθυρο των Windows ή του Clipboard.

Πρέπει να έχουμε σιγουρευτεί για την ύπαρξη εικονιδίων PGP πάνω στην γραμμή εργαλείων της εφαρμογής ηλεκτρονικού ταχυδρομείου.

4.2 Οθόνες του PGP

Οι κύριες οθόνες του PGP είναι:

- οθόνη κλειδιών του PGP
- οθόνη αλληλογραφίας του PGP
- οθόνη διορθωτή δίσκου του PGP

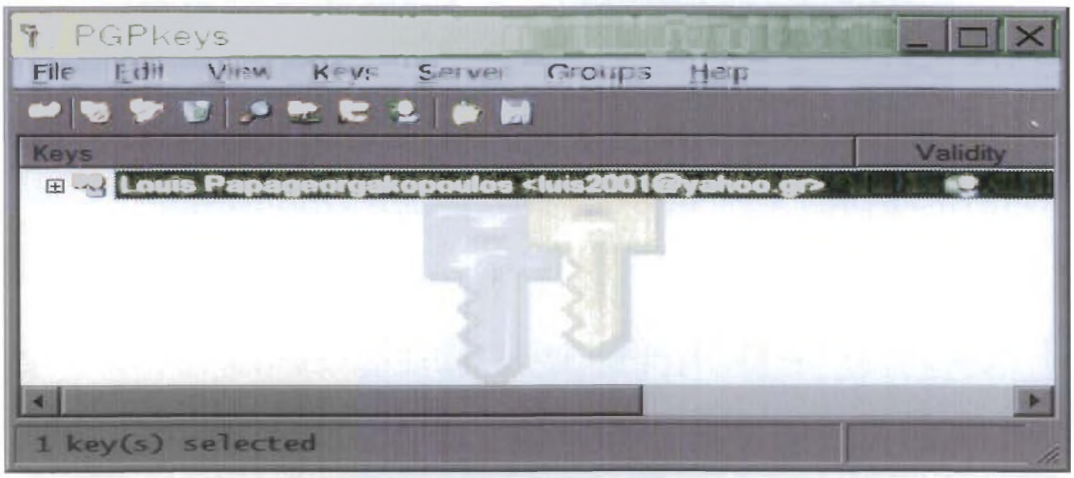
4.2.1 Η οθόνη κλειδιών του PGP

Η οθόνη κλειδιών του PGP μας επιτρέπει την διαχείριση του δικού μας ζεύγους (δημοσίου/ιδιωτικού) κλειδιών, καθώς και τα δημόσια κλειδιά των άλλων. Για να προσπελάσουμε την οθόνη κλειδιών του PGP:

1. Πατάμε το εικονίδιο PGPtray

2. Επιλέγουμε PGPkeys από το μενού

Η οθόνη κλειδιών του PGP εμφανίζεται.



Σχήμα 28: Η οθόνη PGPkeys.

4.2.2 Η οθόνη αλληλογραφίας του PGP (PGPmail)

Η οθόνη αλληλογραφίας του PGP μας δίνει γρήγορη προσπέλαση σε βασικές λειτουργίες του PGP: κρυπτογράφηση, υπογραφή, κρυπτογράφηση και υπογραφή, αποκρυπτογράφηση/επικύρωση, εκκαθάριση, και εκκαθάριση ελεύθερου χώρου. Μπορούμε επίσης να ανοίξουμε την οθόνη κλειδιών του PGP.

Για να προσπελάσουμε την οθόνη αλληλογραφίας του PGP:

1. Πατάμε στο εικονίδιο PGPtray.

2. Επιλέγουμε PGPmail από το μενού.

Η οθόνη αλληλογραφίας του PGP εμφανίζεται.

Σχήμα 29: Η οθόνη PGPmail.

4.2.3 Η οθόνη διορθωτή δίσκου του PGP (Disk Editor)

Η οθόνη του διορθωτή δίσκου του PGP μας επιτρέπει να κάνουμε ενέργειες πάνω στον δίσκο του PGP όπως να αλλάξουμε την κωδική λέξη ή να προσθέσουμε εναλλακτικούς χρήστες.

Μπορούμε να προσπελάσουμε τον διορθωτή δίσκου του PGP κάνοντας τις ακόλουθες ενέργειες:

- Πατάμε το εικονίδιο **PGPtray**, σύρουμε τον κέρσορα πάνω στο **PGPdisk** και μετά στο **Edit Disk.** Πάνω στην επιλογή μίας οθόνης διορθωτή PGP, επιλέγουμε τον δίσκο του PGP που θέλουμε να ανοίξουμε και πατάμε **Open**.
- Από τον εξερευνητή των Windows, δεξί κλικ στον δίσκο PGP που θέλουμε να διορθώσουμε κυλάμε κάτω στο **PGP** και στη συνέχεια **Edit PGPdisk**.

Η οθόνη διορθωτή δίσκου του PGP εμφανίζεται για τον επιλεγμένο δίσκο του PGP.

4.3 Δημιουργώντας ένα ζεύγος κλειδιών και δουλεύοντας με δημόσια κλειδιά

Αυτό το κεφάλαιο περιγράφει τρεις ενέργειες που ο χρήστης θα πρέπει να εκτελέσει για πρώτη φορά μετά την εγκατάσταση του PGP: Δημιουργία του δημοσίου/ιδιωτικού κλειδιού, αποστολή του δημοσίου κλειδιού σε έναν εξυπηρέτη κλειδιών και παραλαβή των δημοσίων κλειδιών άλλων ατόμων από έναν εξυπηρέτη κλειδιών.

Αν έχουμε ήδη ένα ζεύγος δημοσίου/ιδιωτικού κλειδιών και έχουμε εργαστεί με εξυπηρέτες κλειδιών στο παρελθόν τότε θα μπορούσαμε να προσπεράσουμε αυτό το κεφάλαιο.

Τα πεδία αυτού του κεφαλαίου είναι τα εξής:

- Δημιουργία του ζεύγους κλειδιών
- Τοποθέτηση του δημοσίου κλειδιού σε έναν εξυπηρέτη κλειδιών
- Παραλαβή του δημοσίου κλειδιού κάποιου άλλου από τον εξυπηρέτη κλειδιών

4.3.1 **Δημιουργία του ζεύγους κλειδιών**

Για να δημιουργήσουμε ένα νέο ζεύγος κλειδιών:

1. Ανοίγουμε PGPkeys με:

   i. Πατώντας Start → Programs → PGP → PGPkeys

   ii. Πατώντας το εικονίδιο PGPtray () στο Windows System tray και επιλέγουμε **PGPkeys**

   Η οθόνη κλειδιών του PGP απεικονίζει τα ζεύγη κλειδιών που έχουμε δημιουργήσει καθώς επίσης και τα δημόσια κλειδιά των άλλων χρηστών που έχουμε προσθέσει στην

λίστα δημοσίων κλειδιών.

Το PGPkeys είναι το εργαλείο για να διαχειριζόμαστε τις λίστες κλειδιών.

Σημείωση: Ανάλογα με την κατάσταση στην οποία βρισκόμαστε το παράθυρο των κλειδιών PGP μπορεί να είναι κενό, ή να έχει προδιαμορφωθεί από τον διαχειριστή (administrator) του PGP και να απεικονίζει ειδικά κλειδιά.

2. Πατάμε μέσα στη μπάρα μενού των κλειδιών PGP ή κυλίουμε κάτω στο μενού **Keys** και επιλέγουμε **New Key.**

   Το Wizard παραγωγής κλειδιών του PGP μας παρέχει κατευθυντικές πληροφορίες στην πρώτη οθόνη.

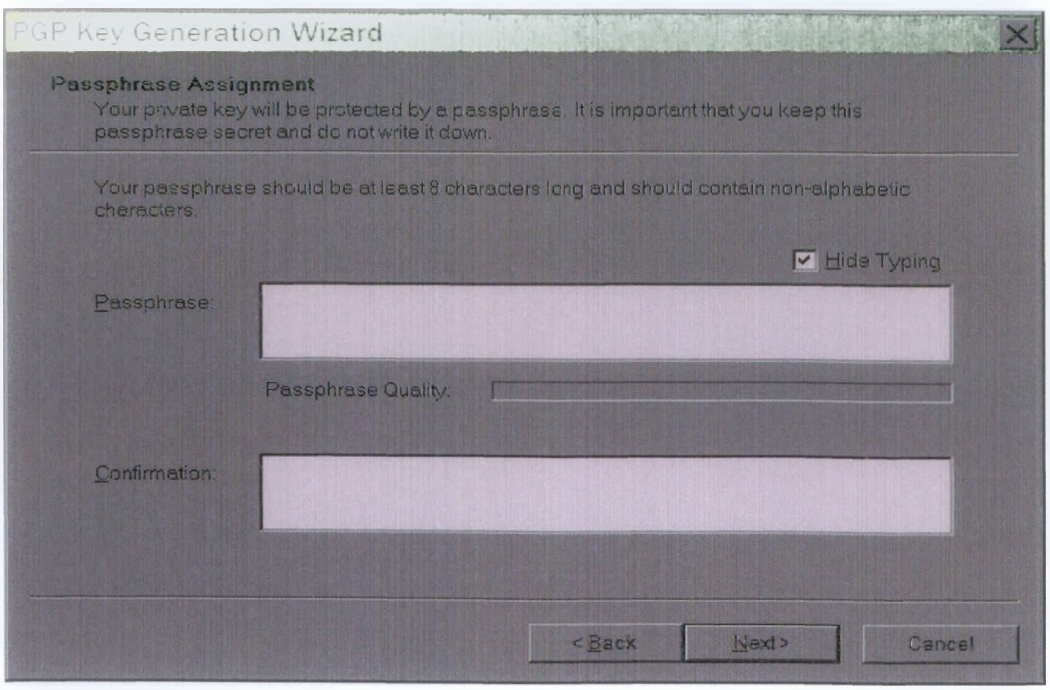
3. Αφού διαβάσουμε την πληροφόρηση πατάμε **Next**.

   Το Wizard παραγωγής κλειδιών PGP μας υποδεικνύει να εισάγουμε το όνομά μας και την διεύθυνση του ηλεκτρονικού ταχυδρομείου.

4. Εισάγουμε το όνομά μας μέσα στο κουτί Full Name και την ηλεκτρονική μας διεύθυνση στο κουτί Email Address και τότε πατάμε Next.

   Δεν είναι υποχρεωτικό να εισάγουμε το πραγματικό μας όνομα ή την ηλεκτρονική μας διεύθυνση. Αν και χρησιμοποιώντας το πραγματικό μας όνομα παρέχουμε την ευκολία στους άλλους να μας αναγνωρίσουν ως τον κάτοχο του δημοσίου κλειδιού μας. Επίσης, με την καταχώρηση της πραγματικής μας ηλεκτρονικής μας διεύθυνσης, μπορούμε τόσο εμείς όσο και οι άλλοι να αποκτήσουμε το πλεονέκτημα του χαρακτηριστικού plug-in, το οποίο ψάχνει αυτόματα το κατάλληλο κλειδί μέσα στην τρέχουσα λίστα κλειδιών όταν αποστέλλουμε αλληλογραφία σε έναν συγκεκριμένο παραλήπτη.

5. Αν το PGP ανιχνεύσει ότι ο υπολογιστής μας βρίσκεται μέσα σε ένα περιβάλλον ανταλλαγής εξυπηρετών της Microsoft, ή αν ο PGP administrator (διαχειριστής) έχει διαμορφώσει το PGP να περιέχει ειδικές ρυθμίσεις εγκατάστασης, τότε εμφανίζεται το πάνελ **Administrator Options**. Αφού διαβάσουμε τις πληροφορίες αυτού του πάνελ πατάμε **Next** για να συνεχίσουμε.



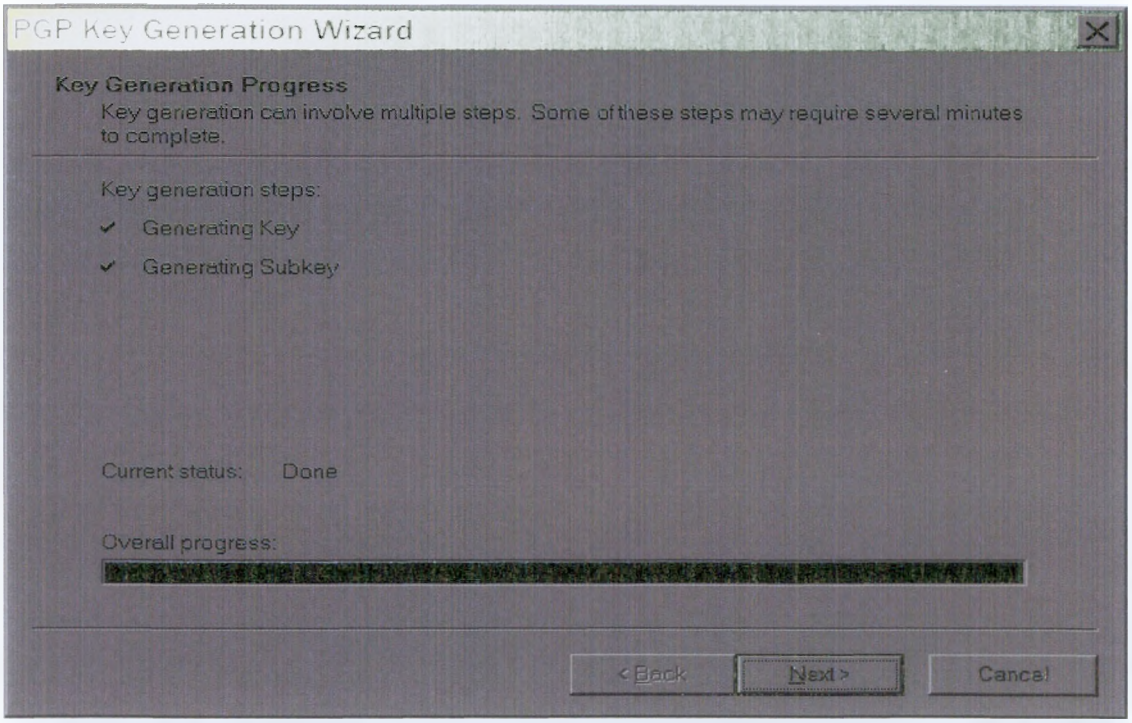
Σχήμα 30: Παραγωγή κλειδιών PGP (εκχώρηση κωδικής φράσης).

6. Πάνω στην οθόνη **Passphrase**, εισάγουμε την συμβολοσειρά από χαρακτήρες ή από λέξεις που θέλουμε να χρησιμοποιούμε για να διατηρούμε αποκλειστική προσπέλαση στο ιδιωτικό μας κλειδί. Για επιβεβαίωση της εισαγωγής, πατάμε Tab όπου μεταπηδάμε στο επόμενο πεδίο και εισάγουμε ξανά την ίδια κωδική λέξη.

   Κανονικά, ως πρόσθετο μέτρο ασφάλειας, οι χαρακτήρες που πληκτρολογούμε για την κωδική λέξη δεν πρέπει να εμφανίζονται στην οθόνη. Αν όμως είμαστε σίγουροι ότι κανείς δεν παρακολουθεί και θέλουμε να βλέπουμε τους χαρακτήρες που τυπώνουμε, τότε πρέπει να καθαρίσουμε το κουτάκι **Hide Typing**.

Προσοχή: Αν και ο administrator έχει αναπτύξει μια πολιτική ανακατασκευής κλειδιών για την εταιρία, κανένας, συμπεριλαμβανομένου και του PGP Corpotation δεν μπορεί να ανακτήσει ένα κλειδί του οποίου έχουμε ξεχάσει την κωδική φράση.

7. Πατάμε **Next** για να ξεκινήσει η διεργασία παραγωγής του κλειδιού.



Σχήμα 31: Η οθόνη διεργασίας παραγωγής κλειδιών PGP

Οι κινήσεις του ποντικιού και το πάτημα των πλήκτρων παράγουν τυχαία πληροφορία που απαιτείται για την δημιουργία ενός μοναδικού ζεύγους κλειδιών. Αν δεν υπάρχει αρκετή τυχαία πληροφορία για την κατασκευή του κλειδιού, εμφανίζεται το πλαίσιο διαλόγου **PGP Random Data**. Όπως είναι εσωτερικά δομημένο μέσα στο πλαίσιο διαλόγου, κινούμε κυκλικά το ποντίκι μας και εισάγουμε μία σειρά από τυχαία πατήματα πλήκτρων μέχρι η μπάρα της διεργασίας να γεμίσει πλήρως.

Αν βρισκόμαστε σε ένα περιβάλλον εναλλαγής εξυπηρέτη της Microsoft, το PGP μας πληροφορεί ότι απαιτείται να ανακτηθεί το user ID του ηλεκτρονικού μας ταχυδρομείου από τον εξυπηρέτη ανταλλαγής και στη συνέχεια να το προσθέσουμε στο νέο κλειδί του PGP.

8. Όταν η διεργασία παραγωγής κλειδιού δείξει ότι ολοκληρώθηκε, πατάμε **Next**.

9. Πατάμε **Finish**.

4.3.2 Τοποθετώντας το δημόσιο κλειδί μας σε έναν εξυπηρέτη κλειδιών

Η καλύτερη μέθοδος για να κάνουμε το δημόσιο κλειδί μας διαθέσιμο, είναι να το τοποθετήσουμε σε έναν δημόσιο εξυπηρέτη κλειδιών, ο οποίος είναι μία μεγάλη βάση δεδομένων από κλειδιά που καθένας μπορεί να προσπελάσει. Με αυτόν τον τρόπο, οι άνθρωποι μπορούν να μας στέλνουν κρυπτογραφημένα μηνύματα χωρίς να πρέπει να παραλάβουν το δημόσιο κλειδί από εμάς.

Για να τοποθετήσουμε το δημόσιο κλειδί μας σε έναν εξυπηρέτη ακολουθούμε τα εξής:

1. Ανοίγουμε τα κλειδιά του PGP

   Η οθόνη PGP Keys εμφανίζεται.

2. Κυλάμε κάτω στο **Server** μενού, επιλέγουμε **Send To**, και καταλήγουμε στον εξυπηρέτη κλειδιών της επιλογής μας.

   Το δημόσιο κλειδί μας φορτώνεται στον εξυπηρέτη κλειδιών που επιλέξαμε.

4.3.3 Λαμβάνοντας δημόσια κλειδιά άλλων από έναν εξυπηρέτη κλειδιών

Προϋπόθεση για την αποστολή ενός κρυπτογραφημένου μηνύματος ηλεκτρονικού ταχυδρομείου σε κάποιον άλλον, είναι η κατοχή του δημοσίου κλειδιού του.

Για να πάρουμε το δημόσιο κλειδί κάποιου από έναν εξυπηρέτη κλειδιών ακολουθούμε τα εξής:

1. Ανοίγουμε τα κλειδιά PGP.

2. Επιλέγουμε **Search** από το μενού **Server** ή πατάμε το κουμπί **Search** μέσα στο PGPkeys.

3. Η οθόνη PGPkeys Search Window εμφανίζεται.

4. Επιλέγουμε τον εξυπηρέτη που επιθυμούμε να κάνουμε αναζήτηση από το **Search for keys on** drop down μενού.

5. Προδιαγράφουμε τα κριτήρια της αναζήτησης

6. Για παράδειγμα: User ID περιέχει John Calt

7. Αυτό πρέπει να βρει τα κλειδιά με το όνομα John Calt μέσα στο δικό τους User ID.

8. Πατάμε **More Choices** για να δώσουμε πρόσθετα κριτήρια στην αναζήτησή μας. Για παράδειγμα, key IDs με το όνομα Susan Jones που δημιουργήθηκαν την 6 Μαρτίου 1982, ή νωρίτερα.

9. Πατάμε **Search**.

10. Εμφανίζεται μια μπάρα διεργασίας απεικονίζοντας την κατάσταση της αναζήτησης. Για ακύρωση της αναζήτησης, πατάμε **Stop Search**.

11. Τα αποτελέσματα της αναζήτησης εμφανίζονται στο παράθυρο.

12. Για να εισάγουμε ένα κλειδί, το σύρουμε από το παράθυρο αναζήτησης πάνω στο παράθυρο κλειδιών PGP και το αφήνουμε εκεί.

13. Μπορούμε να εισάγουμε πολλά κλειδιά την κάθε φορά αν το επιθυμούμε.

14. Κλείνουμε την οθόνη PGPkeys Search Window.

4.4 Ασφάλεια ηλεκτρονικού ταχυδρομείου

Αυτό το κεφάλαιο εξηγεί πώς να διασφαλίζουμε μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνουμε σε άλλους και να αποκρυπτογραφούμε και επικυρώνουμε τα μηνύματα άλλων που στέλνονται σε εμάς.

Στέλνοντας μήνυμα που δεν είναι κρυπτογραφημένο είναι σαν να στέλνουμε ένα γράμμα συμβατικού ταχυδρομείου: το μήνυμα που γράψαμε μπορεί εύκολα να διαβαστεί από κάποιον που βρίσκεται ανάμεσα σε εμάς και τον παραλήπτη.

Για να ασφαλίσουμε το μήνυμα μας, το PGP προσφέρει plug-ins που δουλεύουν μαζί με τις εφαρμογές ηλεκτρονικού ταχυδρομείου και άλλες τυποποιήσεις για να κρυπτογραφήσουν, υπογράψουν, αποκρυπτογραφήσουν και επικυρώσουν ένα κείμενο ηλεκτρονικού ταχυδρομείου. Τα email plug-ins του PGP είναι διαθέσιμα για ενσωμάτωση στα προγράμματα Microsoft Exchange, Outlook and Express, Lotus Notes, Novell Group Wise, και QUALCOMM Eudora.

4.4.1 Κρυπτογράφηση και υπογραφή e-mail

Ο ταχύτερος και ευκολότερος τρόπος για την ασφάλεια των επικοινωνιών ηλεκτρονικού ταχυδρομείου, ικανοποιείται μέσω εφαρμογών που υποστηρίζονται από plug-ins του PGP.

4.4.1.1 Κρυπτογράφηση και υπογραφή μηνυμάτων χρησιμοποιώντας PGP plug-ins

Αν και η διαδικασία ποικίλει ανάμεσα σε διαφορετικές εφαρμογές ηλεκτρονικού ταχυδρομείου, εκτελούμε την διαδικασία της κρυπτογράφησης και υπογραφής με το πάτημα κατάλληλων κουμπιών στη μπάρα εργαλείων της εφαρμογής.

Για κρυπτογράφηση και υπογραφή μέσα από υποστηριζόμενες εφαρμογές ηλεκτρονικού ταχυδρομείου:

1. Χρησιμοποιούμε την εφαρμογή ηλεκτρονικού ταχυδρομείου για να γράψουμε το μήνυμά μας όπως κανονικά θα θέλαμε.

Σημείωση: Εάν στέλνουμε ένα ευαίσθητο μήνυμα, βεβαιωνόμαστε ότι η γραμμή του θέματος φεύγει κενή ή δημιουργώντας μια γραμμή θέματος, αυτή δεν φανερώνει τα περιεχόμενα του κρυπτογραφημένου μηνύματός μας.

2. Όταν έχουμε ολοκληρώσει την συγγραφή του κειμένου του μηνύματος μας, πατάμε το εικονίδιο φάκελος&λουκέτο για να κρυπτογραφήσουμε το κείμενο. Στη συνέχεια πατάμε το εικονίδιο χαρτί&στυλό για να υπογράψουμε το μήνυμά μας.
3. Στέλνουμε το μήνυμά μας όπου θέλουμε.

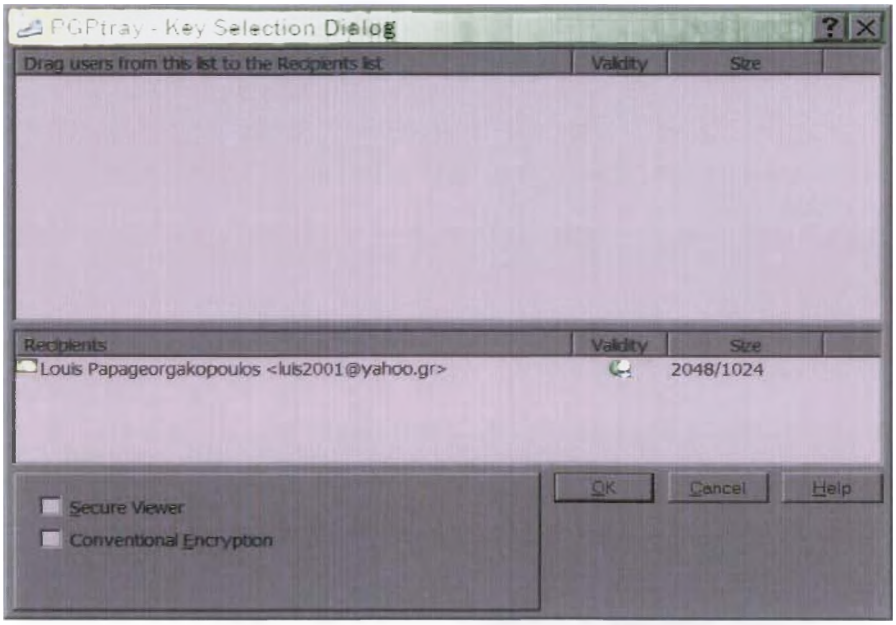
   Εάν έχουμε ένα αντίγραφο από τα δημόσια κλειδιά για κάθε έναν από τους παραλήπτες, τότε χρησιμοποιούνται αυτόματα τα κατάλληλα κλειδιά και το μήνυμα στέλνεται.

   Διαφορετικά, αν έχουμε έναν παραλήπτη του οποίου δεν υπάρχει αντίστοιχο δημόσιο κλειδί, ή ένα ή περισσότερα από τα κλειδιά έχουν μη αποδεκτή εγκυρότητα τότε εμφανίζεται η οθόνη επιλογής παραληπτών του PGP έτσι που να μπορούμε να καθορίσουμε το σωστό κλειδί.

   Μπορούμε να ενισχύσουμε την οθόνη επιλογής παραληπτών, κάνοντάς την να εμφανίζει κάθε φορά που θα έχουμε ένα έγκυρο αντίγραφο από τα δημόσια κλειδιά για κάθε έναν από τους παραλήπτες, κρατώντας πατημένο το πλήκτρο ' Shift ' όταν πατάμε **Send**. Αυτό πρέπει να γίνεται όταν δεν θέλουμε τα μηνύματά μας να στέλνονται αυτόματα και χρησιμοποιούμε το Secure Viewer ή Conventional Encrypt features.
4. Σύρουμε τα δημόσια κλειδιά για αυτούς που πρόκειτε να παραλάβουν ένα αντίγραφο του

κρυπτογραφημένου μηνύματος ηλεκτρονικού ταχυδρομείου, μέσα στο πλαίσιο με τη λίστα των παραληπτών. Μπορούμε επίσης με διπλό κλικ σε κάθε κλειδί να τα μετακινήσουμε από τη μια περιοχή της οθόνης στην άλλη.

Το εικονίδιο Επικύρωσης απεικονίζει το ελάχιστο επίπεδο της εμπιστοσύνης που τα δημόσια κλειδιά στην λίστα παραληπτών είναι έγκυρα. Αυτή η επικύρωση βασίζεται στις υπογραφές που συνδέονται με το κλειδί.



Σχήμα 32: Πλαίσιο διαλόγου επιλογής κλειδιού.

5. Μπορούμε να διαλέξουμε σύμφωνα με τον τύπο των δεδομένων που κρυπτογραφούμε, τις ακόλουθες επιλογές κρυπτογράφησης:

i. **Secure Viewer.** Επιλέγεται για την προστασία των δεδομένων από βίαια επίθεση κατά την αποκρυπτογράφηση. Τα αποκρυπτογραφημένα δεδομένα παρουσιάζονται σε μια ειδική γραμματοσειρά προστασίας από βίαια επίθεση, που είναι μη αναγνώσιμη σε σχέση με τον εξοπλισμό υποκλοπής και επίσης δεν μπορούν να σωθούν σε κρυπτογραφημένη μορφοποίηση.

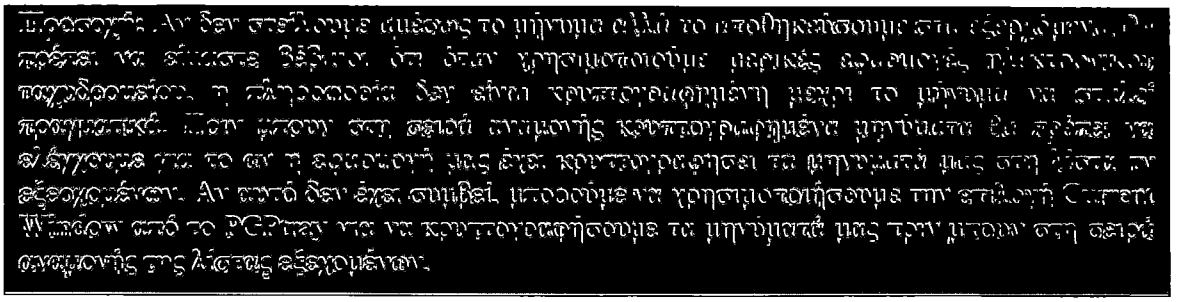
Σημείωση: Η επιλογή Secure Viewer μπορεί να μην είναι συμβατή με προηγούμενες εκδόσεις του PGP. Κρυπτογραφημένα μηνύματα με ενεργοποιημένη αυτή την επιλογή μπορούν να αποκρυπτογραφηθούν από προηγούμενες εκδόσεις του PGP. Αν όχι, αυτό το χαρακτηριστικό θα πρέπει να παραβλεφθεί.

ii. **Conventional Encrypt.** Για τη χρήση μιας κοινής κωδικής φράσης αντί της κρυπτογράφησης δημοσίου κλειδιού. Το μήνυμα κρυπτογραφείται χρησιμοποιώντας ένα κλειδί συνόδου, το οποίο κρυπτογραφεί (και αποκρυπτογραφεί) χρησιμοποιώντας μια κωδική φράση την οποία θα ερωτηθούμε για να καταχωρήσουμε.

6. Πατάμε **OK** να κρυπτογραφηθεί και υπογραφεί το μήνυμα.

Αν έχουμε επιλέξει να υπογράψουμε τα κρυπτογραφημένα δεδομένα, εμφανίζεται η οθόνη Κωδικής λέξης για υπογραφή κλειδιού, που μας ρωτάει για την κωδική φράση πριν το μήνυμα σταλεί.

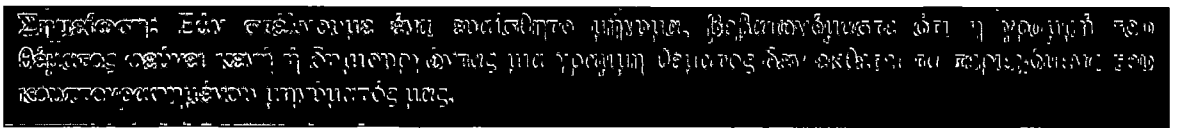
7. Εισάγουμε την κωδική φράση και πατάμε **OK**.



4.4.1.2 Κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου χωρίς υποστήριξη plug-in PGP

Αν η εφαρμογή μας δεν υποστηρίζεται από PGP plug-ins, μπορούμε να χρησιμοποιήσουμε το PGPtray για την κρυπτογράφηση του κειμένου του μηνύματός μας πριν την αποστολή του. Ο ευκολότερος τρόπος είναι μέσω της επιλογής **Current Window** του PGPtray όπως περιγράφεται παρακάτω:

1. Χρησιμοποιούμε την εφαρμογή του ηλεκτρονικού ταχυδρομείου για να συντάξουμε το μήνυμα μας όπως κανονικά θα θέλαμε.



2. Όταν έχουμε ολοκληρώσει τη σύνταξη του κειμένου του μηνύματός μας, πατάμε στο εικονίδιο PGPtray και επιλέγουμε **Encrypt, Sign,** ή **Encrypt & Sign** από το μενού του τρέχοντος παραθύρου.
3. Επιλέγουμε το δημόσιο κλειδί του παραλήπτη του μηνύματος και πατάμε **OK**.

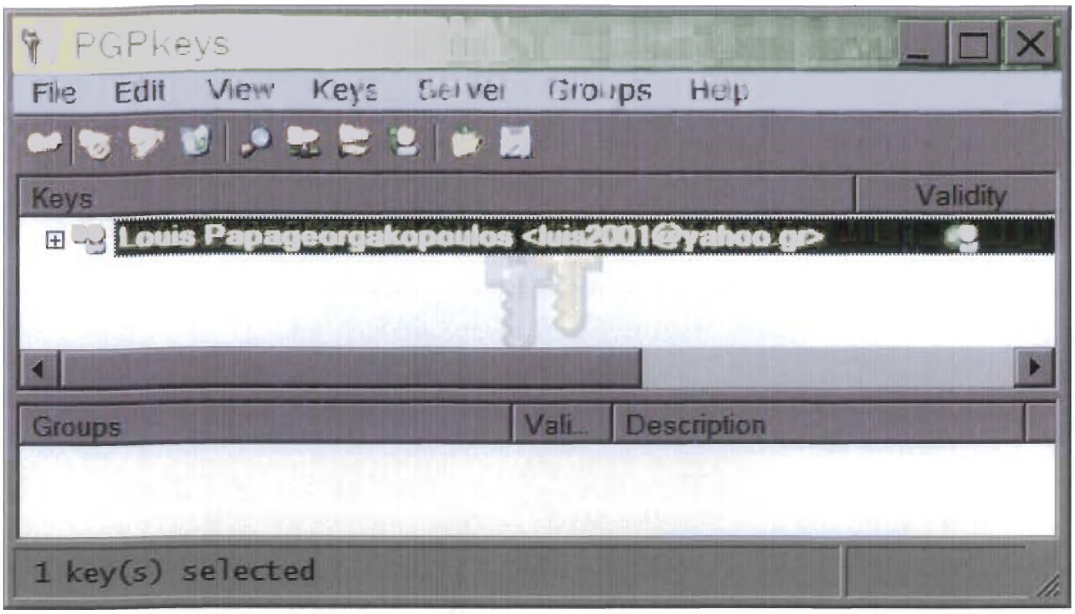
   Εμφανίζεται το κρυπτογραφημένο κείμενο μέσα στο παράθυρο μηνυμάτων του ηλεκτρονικού ταχυδρομείου.
4. Στέλνουμε το μήνυμα όπου φυσικά θέλουμε.

   Αν έχουμε ένα αντίγραφο από τα δημόσια κλειδιά για κάθε έναν από τους παραλήπτες, χρησιμοποιούνται αυτόματα τα κατάλληλα κλειδιά και το μήνυμα στέλνεται.

Τα επόμενα βήματα είναι όμοια με την διαδικασία της κρυπτογράφησης και υπογραφής μηνυμάτων με χρήση PGP plug-ins όπως περιγράφηκε νωρίτερα.

4.4.2 Κρυπτογραφόντας μηνύματα σε ομάδες από παραλήπτες

Μπορούμε να χρησιμοποιήσουμε το PGP για να δημιουργήσουμε λίστες από κατανεμημένες ομάδες. Για παράδειγμα, αν θέλουμε να στείλουμε κρυπτογραφημένη επιστολή σε δέκα άτομα στη διεύθυνση usergroup@pgp.com, θα μπορούσαμε να δημιουργήσουμε μία κατανεμημένη λίστα με αυτό το όνομα. Το μενού των ομάδων μέσα στο PGPkeys περιέχει την επιλογή Show Groups που ενσωματώνει την απεικόνιση του παραθύρου των ομάδων μέσα στο PGPkeys.



Σχήμα 33: Το μενού groups του παραθύρου κλειδιών του PGP.

Σημείωση: Αν πρόκειται να κρυπτογραφήσουμε πληροφορίες σε όλα τα μέλη που αντίκουν σε μια υπάρχουσα κατανεμημένη λίστα ηλεκτρονικού ταχυδρομείου, πρέπει να δημιουργήσουμε μια ομάδα (group) PGP με το ίδιο όνομα η οποία θα περιλαμβάνει τα ίδια μέλη με την κατανεμημένη λίστα του ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, αν υπάρχει μια λίστα τοποθετημένη σε μια εφαρμογή μας ηλεκτρονικού ταχυδρομείου με όνομα [redacted], θα πρέπει να δημιουργήσουμε μια ομάδα με όνομα [redacted] μέσα στο PGP.

4.4.2.1 Δουλεύοντας με κατανεμημένες λίστες

Χρησιμοποιούμε τη δυνατότητα των ομάδων για να δημιουργήσουμε κατανεμημένες λίστες και να τυπώσουμε την λίστα των ατόμων στους οποίους θέλουμε να στείλουμε κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου.

Για να δημιουργήσουμε μία ομάδα (κατανεμημένη λίστα):

1. Επιλέγουμε **New Group** από το μενού **Groups**.

2. Εισάγουμε ένα όνομα για την ομάδα της κατανεμημένης λίστας. Προαιρετικά, εισάγουμε μια περιγραφή για την ομάδα. Για παράδειγμα, μπορούμε να ονομάσουμε την ομάδα "everyone@pgp.com" με περιγραφή "All employees".

3. Πατάμε **OK** για να δημιουργήσουμε την κατανεμημένη λίστα.

   Η λίστα κατανεμημένης ομάδας προστίθεται στην λίστα κλειδιών και μπορεί να αναγνωσθεί μέσα από το Παράθυρο ομάδων (Groups Window).

Για να προσθέσουμε μέλη σε μία κατανεμημένη λίστα:

1. Μέσα στο παράθυρο PGPkeys, επιλέγουμε τους χρήστες ή την λίστα που θέλουμε να προσθέσουμε στην κατανεμημένη λίστα.

2. Σύρουμε τους χρήστες από το παράθυρο PGPkeys στην επιθυμητή κατανεμημένη λίστα μέσα στο παράθυρο Ομάδων.

Σημείωση: Μέλη μιας κατανεμημένης λίστας μπορούν να προστεθούν και σε άλλη κατανεμημένη λίστα.

Για να προσθέσουμε μία κατανεμημένη λίστα σε άλλη κατανεμημένη λίστα:

1. Επιλέγουμε την κατανεμημένη λίστα που θέλουμε να προσθέσουμε σε άλλη λίστα.

2. Σύρουμε την επιλεγμένη λίστα μέσα στην λίστα στην οποία θα προστεθεί.

Για να διαγράψουμε μέλη από μια κατανεμημένη λίστα:

1. Εντός της κατανεμημένης λίστας, επιλέγουμε τα μέλη που θέλουμε να διαγραφούν.

2. Πατάμε **Delete.**

   Το PGP μας ρωτάει για να επικυρώσουμε την επιλογή μας.

Για να διαγράψουμε μια κατανεμημένη λίστα:

1. Επιλέγουμε την κατανεμημένη λίστα που θέλουμε να διαγραφεί από το παράθυρο ομάδων.

2. Πατάμε Delete.

4.4.2.2 Στέλνοντας κρυπτογραφημένα και υπογεγραμμένα μηνύματα σε κατανεμημένες λίστες

Για να στείλουμε κρυπτογραφημένα και υπογεγραμμένα μηνύματα σε μια κατανεμημένη λίστα:

1. Διευθυνσιοδοτούμε την επιστολή στη δική μας κατανεμημένη λίστα επιστολών.

   Το όνομα της κρυπτογραφημένης κατανεμημένης λίστας μας πρέπει να αντιστοιχίσουμε στο όνομα της κατανεμημένης λίστας επιστολών.

2. Χρησιμοποιούμε την εφαρμογή του ηλεκτρονικού ταχυδρομείου για να συντάξουμε τα μηνύματά μας όπως φυσικά θα θέλαμε.

3. Όταν έχουμε ολοκληρώσει την σύνταξη του κειμένου από το μήνυμα, πατάμε πάνω στο εικονίδιο PGPtray και επιλέγουμε **Encrypt, Sign** ή **Encrypt & Sign** από το μενού του τρέχοντος παραθύρου.

   Εμφανίζεται η οθόνη παραληπτών PGP Key Recipients.

4. Επιλέγουμε τα δημόσια κλειδιά των παραληπτών για το κείμενο που κρυπτογραφούμε ή υπογράφουμε.

5. Στέλνουμε το μήνυμα.

4.4.3 Αποκρυπτογράφηση και επικύρωση μηνύματος

Ο ταχύτερος και ευκολότερος τρόπος για την ασφάλεια των επικοινωνιών ηλεκτρονικού ταχυδρομείου είναι η χρήση εφαρμογής που υποστηρίζεται από plug-ins του PGP. Αν χρησιμοποιούμε μια εφαρμογή ηλεκτρονικού ταχυδρομείου που δεν υποστηρίζεται από plug-ins του PGP, μπορούμε να κρυπτογραφήσουμε, υπογράψουμε, αποκρυπτογραφήσουμε και επικυρώσουμε το κείμενο του μηνύματός μας χρησιμοποιώντας το PGPtray.

4.4.3.1 Αποκρυπτογραφώντας και επικυρώνοντας μηνύματα χρησιμοποιώντας plug-ins του PGP

Αν και η διαδικασία ποικίλει ανάμεσα σε διαφορετικές εφαρμογές ηλεκτρονικού ταχυδρομείου, όταν χρησιμοποιούμε μια τέτοια εφαρμογή υποστηριζόμενη από plug-ins, μπορούμε να προτιμήσουμε τις λειτουργίες της αποκρυπτογράφησης και επικύρωσης με το πάτημα του εικονιδίου ανάπτυξης μέσα στο μήνυμα ή στην γραμμή εργαλείων της εφαρμογής. Σε μερικές περιπτώσεις μπορεί να χρειαστεί να επιλέξουμε αποκρυπτογράφηση/επικύρωση από το μενού εντός της εφαρμογής του ηλεκτρονικού ταχυδρομείου. Επιπρόσθετα, αν χρησιμοποιήσουμε μια εφαρμογή που υποστηρίζει το πρότυπο PGP/MIME, μπορούμε να αποκρυπτογραφήσουμε και επικυρώσουμε τα μηνύματα

επίσης, για κάθε αρχείο που συνδέεται με πάτημα ενός εικονιδίου προσαρτημένου στο μήνυμά μας.

Εάν χρησιμοποιούμε μία εφαρμογή που δεν υποστηρίζεται από plug-ins του PGP, θα αποκρυπτογραφήσουμε και επικυρώσουμε τα μηνύματά μας μέσω του PGPtray. Επιπρόσθετα, αν το μήνυμά μας περιλαμβάνει κρυπτογραφημένης επισύναψης αρχείο, τότε θα πρέπει να το αποκρυπτογραφήσουμε ξεχωριστά μέσω του PGPtray.

Για να αποκρυπτογραφήσουμε και επικυρώσουμε από υποστηριζόμενες εφαρμογές ηλεκτρονικού ταχυδρομείου:

1. Ανοίγουμε το εισερχόμενο κρυπτογραφημένο μήνυμα.

   Θα δούμε ένα μπλοκ μη αναγνώσιμο κρυπτογραφημένο κείμενο μέσα στο σώμα του μηνύματος.

2. Για αποκρυπτογράφηση και επικύρωση του μηνύματος πατάμε το εικονίδιο κλειδωμένου φάκελου.

   Για αποκρυπτογράφηση και επικύρωση συνδεόμενων αρχείων, τα αποκρυπτογραφούμε ξεχωριστά χρησιμοποιώντας το εικονίδιο PGPtray.

   Εμφανίζεται η οθόνη εισαγωγής της κωδικής φράσης του PGP, που μας ζητάει να εισάγουμε την κωδική φράση.

3. Εισάγουμε την κωδική φράση και πατάμε **OK**.

   Το μήνυμα είναι αποκρυπτογραφημένο. Αν αυτό έχει υπογραφεί και έχουμε το δημόσιο κλειδί του αποστολέα, εμφανίζεται ένα μήνυμα που υποδεικνύει πότε επικυρώθηκε η υπογραφή.

   Αν το μήνυμα είναι κρυπτογραφημένο με ενεργοποιημένη την επιλογή του Secure Viewer, ένα συμβουλευτικό μήνυμα εμφανίζεται. Πατάμε **OK** για να συνεχίσουμε. Το αποκρυπτογραφημένο μήνυμα εμφανίζεται σε μια ασφαλή οθόνη του PGP μέσα σε ένα ειδική γραμματοσειρά προστασίας από βίαιη επίθεση.

4. Μπορούμε να σώσουμε το μήνυμα στην αποκρυπτογραφημένη του κατάσταση, ή μπορούμε να το διατηρήσουμε στην αυθεντική κρυπτογραφημένη έκδοση πράγμα που σημαίνει ασφάλεια.

Στιγμιότυπα: Μηνύματα κρυπτογραφημένα με ενεργοποιημένη την επιλογή Secure Viewer, δεν μπορούν να σωθούν στην αποκρυπτογραφημένη τους κατάσταση

4.4.3.2 Αποκρυπτογραφώντας και επικυρώνοντας μηνύματα χωρίς υποστήριξη plug-in PGP

Αν η εφαρμογή ηλεκτρονικού ταχυδρομείου δεν υποστηρίζεται από PGP plug-ins, μπορούμε να χρησιμοποιήσουμε το PGPtray για να αποκρυπτογραφήσουμε το κείμενο του μηνύματος πριν το στείλουμε. Ο ευκολότερος τρόπος είναι μέσω της χρήσης της επιλογής του τρέχοντος παραθύρου στο PGPtray.

Για αποκρυπτογράφηση και επικύρωση από μη-υποστηριζόμενες εφαρμογές ηλεκτρονικού ταχυδρομείου:

1. Ανοίγουμε το εισερχόμενο κρυπτογραφημένο μήνυμα.

   Θα δούμε ένα μπλοκ από μη αναγνώσιμο κρυπτογραφημένο κείμενο μέσα στο σώμα του μηνύματος.

2. Στο PGPtray επιλέγουμε Current Window → Decrypt/Verify.

   Αν το μήνυμα περιλαμβάνει επισυναπτόμενο κρυπτογραφημένου αρχείου, το αποκρυπτογραφούμε ξεχωριστά με το PGPtools ή PGPtray.

Εμφανίζεται η οθόνη εισαγωγής της κωδικής φράσης του PGP ζητώντας μας να εισάγουμε την κωδική μας φράση.

3. Εισάγουμε την κωδική μας φράση και πατάμε **OK**.

   Το μήνυμα είναι αποκρυπτογραφημένο. Αν αυτό έχει υπογραφεί, εμφανίζεται ένα μήνυμα που απεικονίζει πότα έχει επικυρωθεί η υπογραφή.

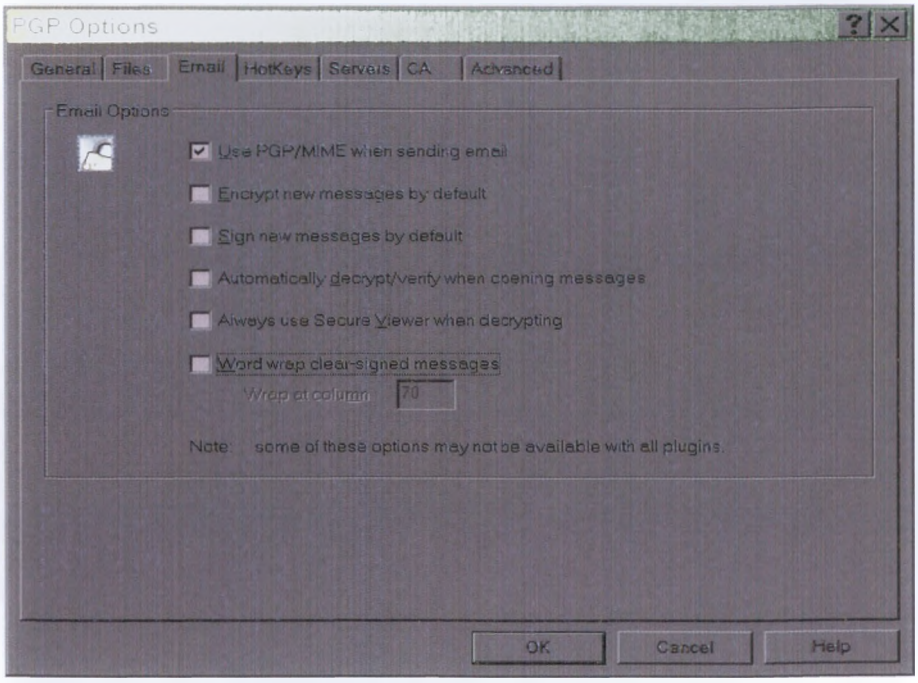
   Αν το μήνυμα είναι κρυπτογραφημένο με ενεργοποιημένη την επιλογή του Secure Viewer, ένα συμβουλευτικό μήνυμα εμφανίζεται. Πατάμε **OK** για να συνεχίσουμε. Το αποκρυπτογραφημένο μήνυμα εμφανίζεται σε μια ασφαλή οθόνη του PGP μέσα σε ένα ειδική γραμματοσειρά προστασίας από βίαιη επίθεση.

4. Μπορούμε να σώσουμε το μήνυμα στην αποκρυπτογραφημένη του κατάσταση, ή μπορούμε να το διατηρήσουμε στην αυθεντική κρυπτογραφημένη έκδοση πράγμα που σημαίνει ασφάλεια.

Σημειωση: Μηνύματα κρυπτογραφημένα με ενεργοποιημένη την επιλογή Secure Viewer. δεν μπορούν να σωθούν στην αποκρυπτογραφημένη τους κατάσταση.

4.4.4 PGP/MIME

Αν χρησιμοποιούμε μια εφαρμογή ηλεκτρονικού ταχυδρομείου μαζί με ένα από τα plug-ins που υποστηρίζει το πρότυπο PGP/MIME και επικοινωνούμε με άλλους χρήστες των οποίων οι εφαρμογές ηλεκτρονικού ταχυδρομείου επίσης υποστηρίζονται από αυτό το πρότυπο τότε και οι δύο μπορούμε αυτόματα να κρυπτογραφούμε και αποκρυπτογραφούμε τα μηνύματά μας και κάθε προσαρτημένο αρχείο όταν στέλνουμε ή ανακτούμε τις επιστολές μας. Όλα όσα έχουμε να κάνουμε ενεργοποιούνται στις λειτουργίες κρυπτογράφησης και υπογραφής του PGP/MIME από την καρτέλα Email της οθόνης PGP Options, η οποία μπορεί να ανοιχτεί από το PGPtray ή μέσα από το PGPkeys.



Σχήμα 34: Ενεργοποίηση του PGP/MIME.

Όταν παραλαμβάνουμε μήνυμα από κάποιον ο οποίος χρησιμοποιεί τη δυνατότητα PGP/MIME το μήνυμα φτάνει μαζί με μία εικόνα στο παράθυρο μηνύματος που απεικονίζει ότι είναι κωδικοποίησης PGP/MIME.

Για να αποκρυπτογραφήσουμε το κείμενο και επισυνάψεις αρχείων που είναι ενσωματωμένα σε PGP/MIME μήνυμα ηλεκτρονικού ταχυδρομείου και για να επικυρώσουμε όποιες ψηφιακές υπογραφές, απλά πατάμε το εικονίδιο στυλό/λουκέτο. Οι επισυνάψεις αρχείων είναι ακόμα κρυπτογραφημένες αν δεν έχει χρησιμοποιηθεί το PGP/MIME, αλλά η διεργασία της αποκρυπτογράφησης είναι πιο περίπλοκη για τον παραλήπτη.

Όταν κρυπτογραφούμε και υπογράφουμε μέσα από μια εφαρμογή ηλεκτρονικού ταχυδρομείου που υποστηρίζεται από plug-ins του PGP, έχουμε δύο επιλογές που εξαρτώνται από τον τύπο της εφαρμογής ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί ο παραλήπτης. Αν επικοινωνούμε με άλλους χρήστες PGP που η εφαρμογή τους υποστηρίζεται από το πρότυπο PGP/MIME, μπορούμε να αποκτήσουμε τα πλεονεκτήματα της κρυπτογράφησης και υπογραφής των μηνυμάτων ηλεκτρονικού ταχυδρομείου καθώς και κάθε επισύναψης αρχείου κατά την αποστολή τους. Αν επικοινωνούμε με κάποιον που η εφαρμογή του δεν είναι συμβατή με το PGP/MIME, τότε θα πρέπει να κρυπτογραφήσουμε με το PGP/MIME απενεργοποιημένο για να αποφύγουμε προβλήματα συμβατότητας.

Παραπέμπουμε στον παρακάτω αναλυτικό πίνακα με τα plug-ins και τα χαρακτηριστικά τους:

	Eudora	**Outlook**	**Outlook Express**	**Lotus Notes**	**Novell GroupWise**
PGP/MIME	Ναι	Όχι	Όχι	Όχι	Όχι
Auto-decrypt	Όχι	Ναι	Ναι	Ναι	Ναι
Encrypt HTML	Ναι	Ναι	Όχι	Ναι	Όχι
Preserve text formatting	Ναι	Ναι	Όχι	Ναι	Όχι
Encrypt attachments	Ναι	Ναι	Όχι	Ναι	Ναι
Encrypt/Sign defaults	Ναι	Ναι	Ναι	Ναι	Ναι
Print decrypted email	Ναι	Ναι	Όχι	Ναι	Όχι

Σχήμα 35: Πίνακας των plug-ins με τα χαρακτηριστικά τους.

4.5 Ρυθμίζοντας τα χαρακτηριστικά του PGP (PGP options)

Αυτό το κεφάλαιο περιγράφει πώς να στήσουμε το τα χαρακτηριστικά του PGP στο επιμέρους υπολογιστικό περιβάλλον.

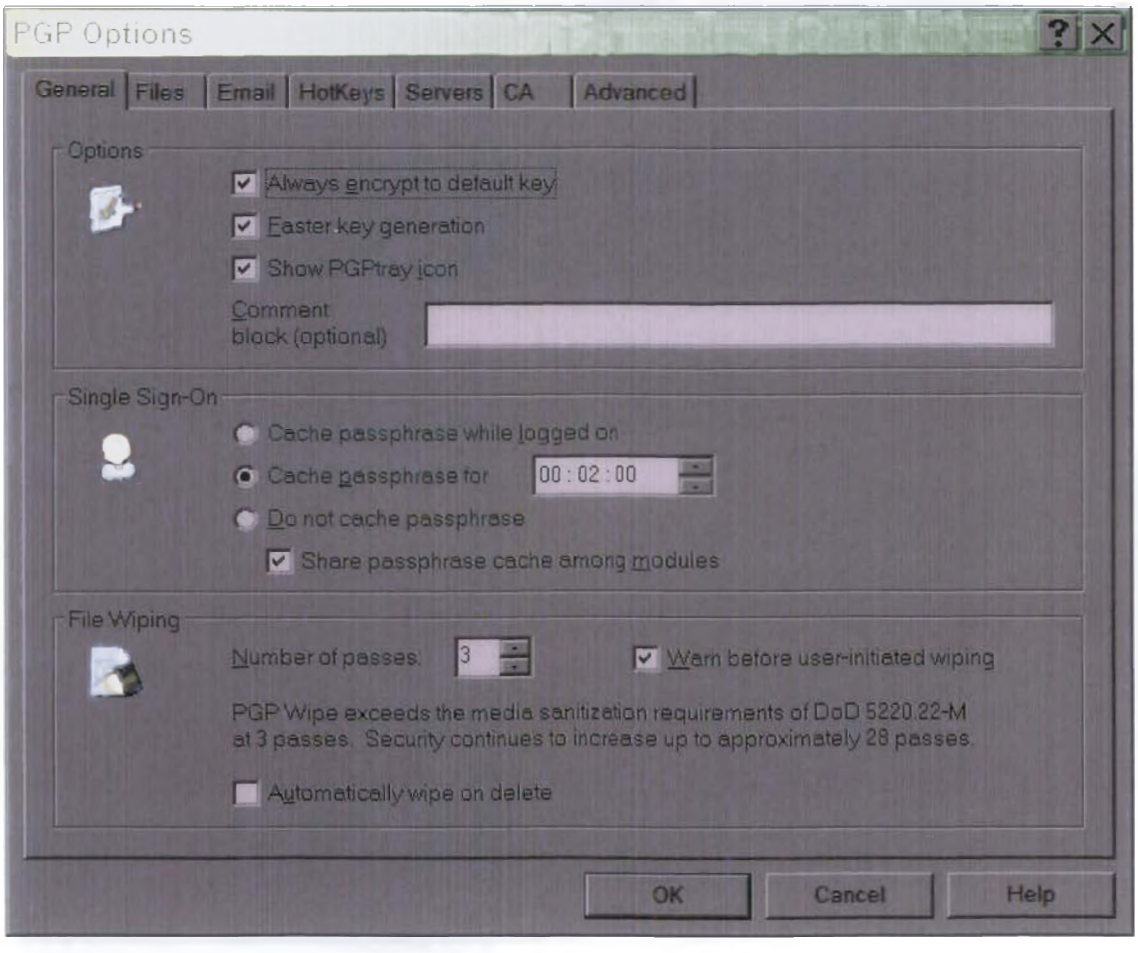
4.5.1 Ρυθμίζοντας γενικά χαρακτηριστικά

Χρησιμοποιούμε την επιλογή **General** για να καθορίσουμε προαιρετικά, απλή sign-on, και επιλογές διαγραφής αρχείων.

Έτσι κάνουμε τις επιλογές μας για τις παρακάτω δυνατότητες:

- Πάντα κρυπτογράφηση με το προκαθορισμένο κλειδί: Όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα αρχεία που έχουμε κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη, είναι επίσης κρυπτογραφημένα στο μηχάνημά μας με το προκαθορισμένο δημόσιο κλειδί. Είναι χρήσιμο να θέσουμε αυτή την επιλογή ενεργή με συνέπεια να έχουμε τη δυνατότητα της αποκρυπτογράφησης των περιεχομένων κάθε μηνύματος ή αρχείου που κρυπτογραφούμε.
- Ταχύτερη παραγωγή κλειδιού: Όταν επιλέγεται αυτή η ρύθμιση, απαιτείται λιγότερος χρόνος για την δημιουργία ενός νέου ζεύγους κλειδιών Diffie-Hellman/DSS. Αυτή η διαδικασία γίνεται ταχύτερη, με την χρήση ενός συνόλου από πρώτους αριθμούς υπολογισμένους από πριν, διεργασία που είναι προτιμότερη σε σχέση με την κατανάλωση χρόνου της δημιουργίας τους από την αρχή κάθε φορά που παράγεται ένα νέο κλειδί. Ωστόσο, δεν πρέπει να ξεχνάμε ότι η ταχεία παραγωγή κλειδιού υλοποιείται μόνο για μεγέθη πάνω από 1024 και κάτω από 4096 bits. Αυτό αποκλείει την πιθανότητα σε οποιονδήποτε βασίζεται στη γνώση αυτών των πρώτων αριθμών να σπάσει το κλειδί. Ωστόσο, κάποιοι προτιμούν να ξοδέψουν τον επιπλέον χρόνο για τη δημιουργία ενός ζεύγους κλειδιών με το μέγιστο επίπεδο ασφάλειας.

  Η γενική αντίληψη στην κρυπτογραφική κοινωνία είναι ότι η χρήση εγγεγραμμένων στο σκληρό δίσκο πρώτων αριθμών παρέχει ασφάλεια στους αλγόριθμους Diffie-Hellman/DSS. Αν αυτό το χαρακτηριστικό μας προκαλεί δυσφορία τότε το απενεργοποιούμε.



Σχήμα 36: Γενικές επιλογές του PGP.

- Εμφάνιση του εικονιδίου PGPtray: Όταν το κουτάκι ελέγχου είναι επιλεγμένο, έχουμε πρόσβαση σε πολλές χρήσιμες λειτουργίες του PGP διαμέσου της ευκολίας του PGPtray.
- Πλαίσιο σχολείων: Μπορούμε να προσθέσουμε ένα κείμενο σχολείων σε αυτήν τη περιοχή. Το κείμενο που θα εισάγουμε εδώ, θα περιλαμβάνεται πάντοτε στα μηνύματα και τα αρχεία που έχουμε κρυπτογραφήσει ή υπογράψει. Τα σχόλια εισάγονται σε αυτό το πεδίο εμφανίζουν παρακάτω το --ΑΡΧΙΚΟ ΠΛΑΙΣΙΟ ΜΗΝΥΜΑΤΟΣ PGP--, επικεφαλίδα κειμένου και αριθμό έκδοσης του κάθε μηνύματος.
- Απόκρυψη της κωδικής φράσης κατά την σύνδεση: Σώζει αυτόματα την κωδική φράση στην μνήμη μέχρι να αποσυνδεθεί ο υπολογιστής. Αν επιλέξουμε αυτή την δυνατότητα, τότε θα υποβάλλουμε την κωδική φράση μία φορά για κάθε αρχική υπογραφή και εργασία αποκρυπτογράφησης. Δεν θα χρειαστεί να υποβληθεί ξανά για την ίδια εργασία μέχρι την αποσύνδεση του υπολογιστή.

Προσοχή: Όταν αυτή η ρύθμιση επιλέγεται, είναι πολύ σημαντικό να αποσυνδέσουμε τον υπολογιστή μας πριν τον εγκαταλείψουμε από την παρακολούθησή μας. Η κωδική λέξη μπορεί να διατηρηθεί κρυμμένη για εβδομάδες αν δεν έχουμε συνδεθεί καθόλου στο διάστημα αυτό, κανείς δεν μπορεί να διαβάσει τα κρυπτογραφημένα μηνύματα ή να κρυπτογραφήσει μηνύματα από τον υπολογιστή μας χωρίς να βρίσκεστε μακριά από τον υπολογιστή μας.

- Κρυμμένη κωδική φράση για καθορισμένο χρόνο: Σώζει αυτόματα την κωδική φράση στην μνήμη για καθορισμένη χρονική διάρκεια (σε ώρες, λεπτά, δευτερόλεπτα). Αν επιλέξουμε αυτή τη δυνατότητα τότε θα υποβάλλουμε την κωδική φράση μία φορά για κάθε αρχική υπογραφή και εργασία αποκρυπτογράφησης. Δεν θα χρειαστεί να υποβληθεί ξανά μέχρι την παρέλευση του χρόνου που καθορίσαμε. Η προκαθορισμένη ρύθμιση είναι 2 λεπτά.
- Χωρίς απόκρυψη της κωδικής φράσης: Όταν επιλέξουμε αυτή την ρύθμιση, η κωδική φράση δεν αποθηκεύεται στην μνήμη για κάποιο χρονικό διάστημα. Συνεπώς θα πρέπει να εισάγουμε την κωδική φράση για όλες τις δικτυακές επικοινωνίες του PGP, τόσο κατά την κρυπτογράφηση, την υπογραφή και την αποκρυπτογράφηση.
- Διανομή κωδικής φράσης μεταξύ modules: Σώζει αυτόματα την κωδική φράση στην μνήμη και την διανέμει ανάμεσα σε άλλα PGP modules. Για παράδειγμα, αν εισάγουμε την κωδική μας φράση για υπογραφή, δεν μας υπαγορεύει να την χρησιμοποιήσουμε αργότερα για την αποκρυπτογράφηση. Ενεργοποιούμε αυτή την επιλογή μαζί με απόκρυψη της κωδικής φράσης, όταν η επιλογή logged on και η κωδική φράση έχουν αποθηκευτεί στην μνήμη εώς να σβήσουμε τον υπολογιστή μας. Επίσης την ενεργοποιούμε, όταν θέλουμε να καθορίσουμε την διάρκεια στην οποία θέλουμε να σώσουμε την κωδική μας φράση.
- Αριθμός διελεύσεων: Αυτή η ρύθμιση ελέγχει πόσες φορές η δυνατότητα σβησίματος μπορεί να εφαρμοστεί πάνω στον δίσκο.
- Προειδοποίηση πριν ο χρήστης ξεκινήσει το σβήσιμο: Όταν αυτή η επιλογή ενεργοποιείται, πριν να σβήσιμο ένα αρχείο εμφανίζεται το πλαίσιο διαλόγου που μας δίνει την τελευταία ευκαιρία να αλλάξουμε την προθεσή μας πριν το PGP διαγράψει τα περιεχόμενα του αρχείου από τον υπολογιστή μας.
- Αυτόματο σβήσιμο κατά την διαγραφή: Όταν διαγράφουμε ένα αρχείο κανονικά με την τοποθέτησή του στον κάδο ανακύκλωσης, το όνομα του αρχείου αφαιρείται από τον κατάλογο αρχείων, αλλά τα δεδομένα παραμένουν στον δίσκο και είναι ακόμα ανακτήσιμα και μετά το άδειασμα στον κάδο ανακύκλωσης. Όταν ενεργοποιήσουμε αυτή την επιλογή, αδειάζοντας τον κάδο ανακύκλωσης, τότε σβήνουν τα περιεχόμενα και δεν μπορούν να ανακτηθούν.

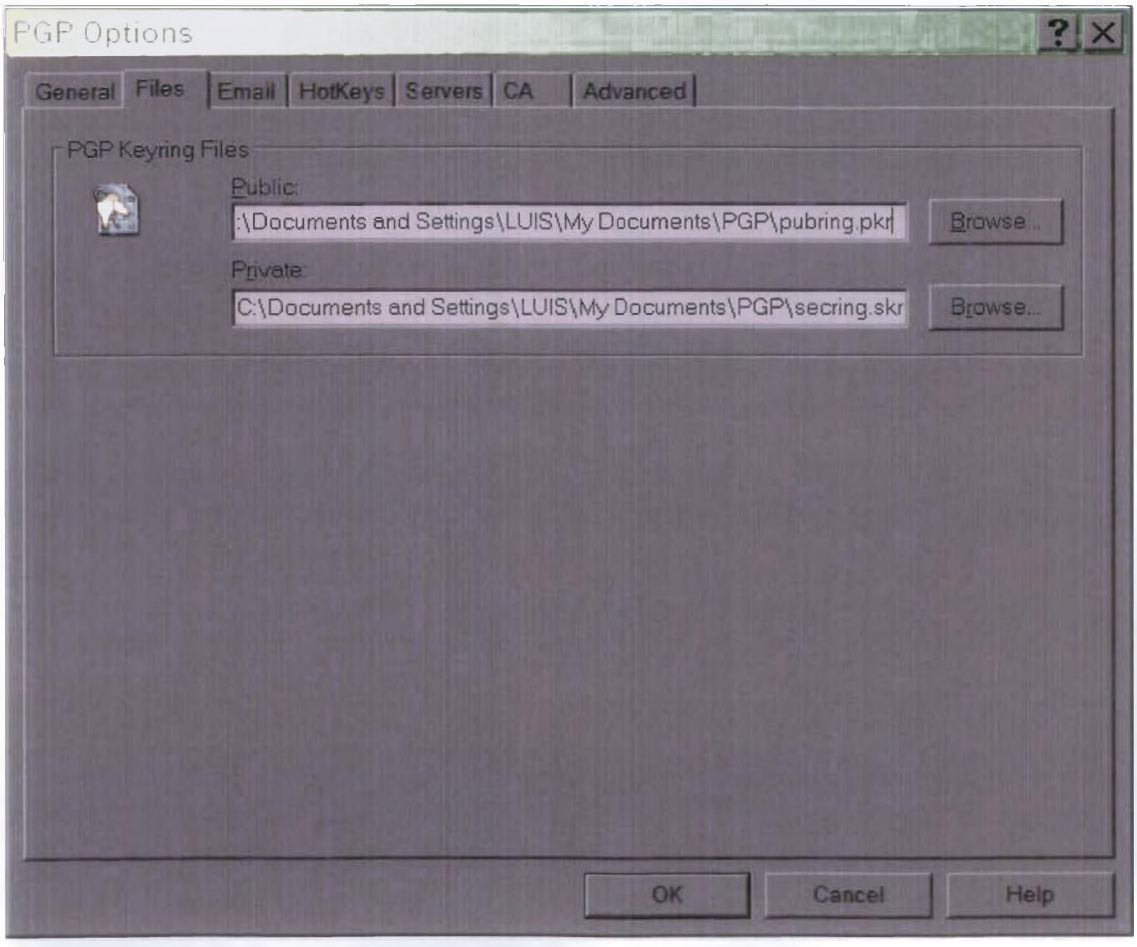
Πατάμε **OK** για να σώσουμε τις αλλαγές.

4.5.2 Ρυθμίζοντας τα χαρακτηριστικά αρχείου

Χρησιμοποιούμε την καρτέλα **Files** για να προσδιορίσουμε την θέση στις λίστες κλειδιών που χρησιμοποιούνται για αποθήκευση του ιδιωτικού και δημοσίου κλειδιού μας. Κάνουμε τις επιλογές μας για τις ακόλουθες δυνατότητες:

- **Public:** δείχνει την τρέχουσα θέση και όνομα του αρχείου όπου το πρόγραμμα του PGP αναμένει να βρει τις λίστες δημοσίων κλειδιών μας. Αν σκοπεύουμε να τοποθετήσουμε τα δημόσια κλειδιά σε κάποια άλλη τοποθεσία, πρέπει να προσδιορίσουμε εδώ αυτή την πληροφορία. Αυτή η τοποθεσία μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση όλων των αυτόματων backups στις λίστες δημοσίων κλειδιών.
- **Private:** δείχνει την τρέχουσα θέση και όνομα του αρχείου όπου το πρόγραμμα του PGP αναμένει να βρει τις λίστες ιδιωτικών κλειδιών μας. Αν σκοπεύουμε να τοποθετήσουμε τα δημόσια κλειδιά σε κάποια άλλη τοποθεσία, πρέπει να προσδιορίσουμε εδώ αυτή την πληροφορία. Κάποιοι χρήστες προτιμούν να κρατάνε τα ιδιωτικά τους κλειδιά σε μια δισκέτα, την οποία εισάγουν κάθε φορά που θέλουν να υπογράψουν ή να αποκρυπτογραφήσουν μηνύματα. Αυτή η τοποθεσία μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση όλων των αυτόματων backups στις λίστες δημοσίων κλειδιών.

Πατάμε **OK** για να σωθούν οι αλλαγές.



Σχήμα 37: Επιλογές αρχείου του PGP.

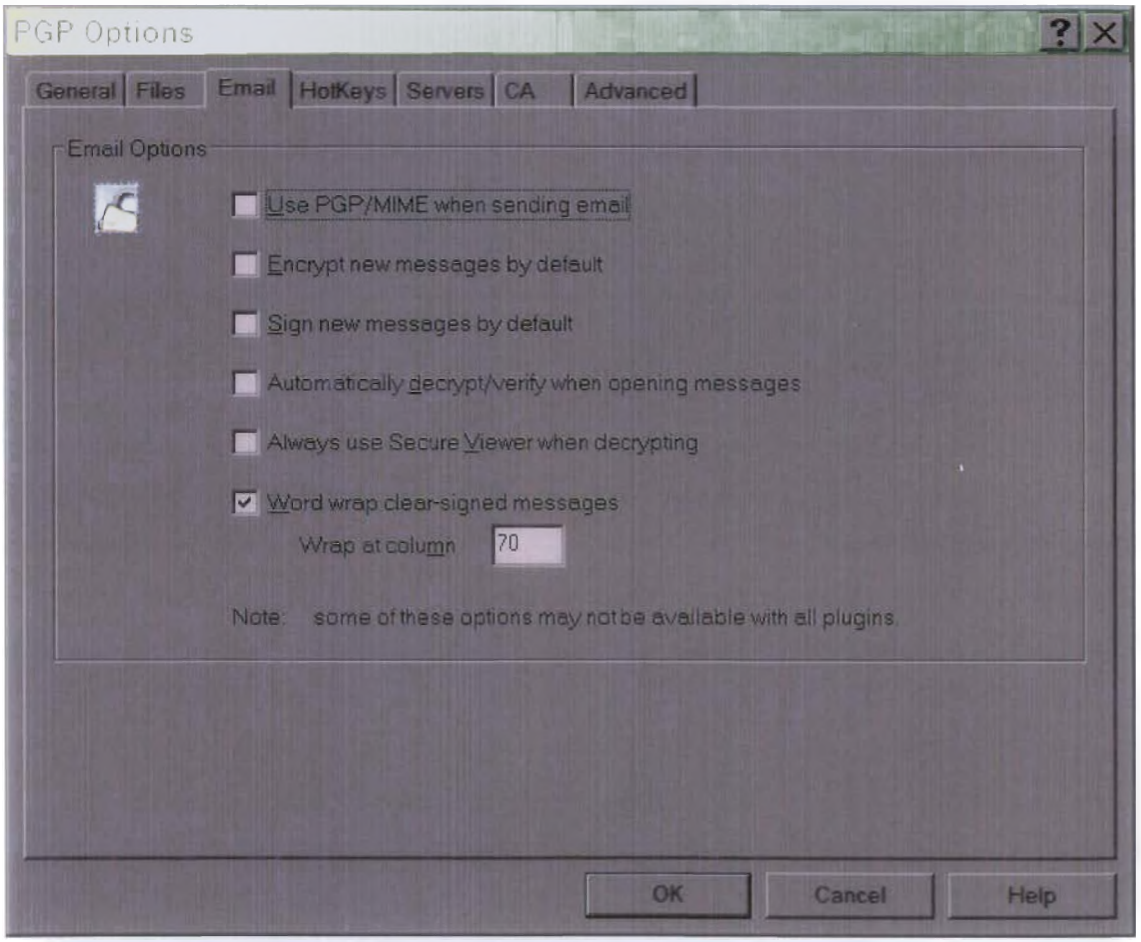
4.5.3 Ρυθμίζοντας τα χαρακτηριστικά του ηλεκτρονικού ταχυδρομείου

Χρησιμοποιούμε την καρτέλα **Email** για να προδιαγράψουμε ρυθμίσεις στις εφαρμογές

ηλεκτρονικού ταχυδρομείου. Δεν εφαρμόζονται όλες οι παρακάτω επιλογές σε κάθε εφαρμογή ηλεκτρονικού ταχυδρομείου.

Κάνουμε τις επιλογές μας για τις παρακάτω δυνατότητες:

- **Use PGP/MIME when sending mail:** Μόνο αν χρησιμοποιούμε το Eudora plug-in και έχουμε ενεργοποιημένη αυτή την ρύθμιση, τότε όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι επισυνάψεις αρχείων είναι αυτόματα κρυπτογραφημένα στον προοριζόμενο παραλήπτη. Αυτή η ρύθμιση δεν έχει αποτελέσματα στις κρυπτογραφήσεις που εκτελούμε από το Clipboard. Κάποιες εφαρμογές ηλεκτρονικού ταχυδρομείου δεν υποστηρίζουν αυτή την δυνατότητα.
- **Encrypt new messages by default:** Αν ενεργοποιήσουμε αυτή την ρύθμιση, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα προσαρτημένα αρχεία κρυπτογραφούνται αυτόματα. Κάποιες εφαρμογές ηλεκτρονικού ταχυδρομείου δεν υποστηρίζουν αυτή την δυνατότητα.



Σχήμα 38: Επιλογές ηλεκτρονικού ταχυδρομείου του PGP.

- **Sign new messages by default.** Αν ενεργοποιήσουμε αυτή την ρύθμιση, υποβαλλόμαστε να υπογράψουμε όλα μας τα μηνύματα ηλεκτρονικού ταχυδρομείου. Κάποιες εφαρμογές ηλεκτρονικού ταχυδρομείου δεν υποστηρίζουν αυτή την δυνατότητα. Αυτή η ρύθμιση δεν έχει αποτέλεσμα σε άλλες υπογραφές που προσθέτουμε από το Clipboard ή μέσα από τον Windows Explorer.
- **Automatically decrypt/verify when opening messages.** Αν ενεργοποιήσουμε αυτή την ρύθμιση, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα προσαρτημένα αρχεία που είναι κρυπτογραφημένα και/ή υπογεγραμμένα, αποκρυπτογραφούνται και επικυρώνονται

αυτόματα. Κάποιες εφαρμογές ηλεκτρονικού ταχυδρομείου δεν υποστηρίζουν αυτή την δυνατότητα.

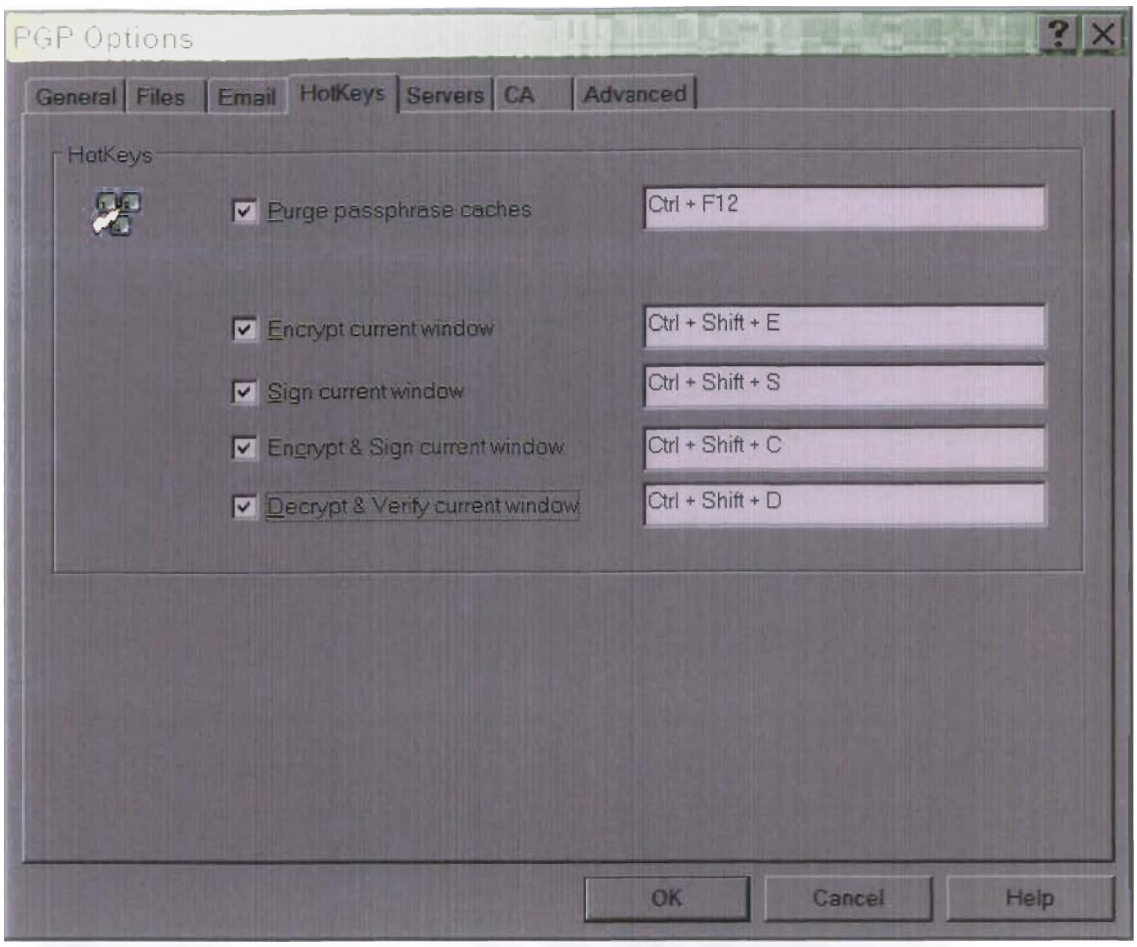
- **Always use Secure Viewer when decrypting:** Αν ενεργοποιήσουμε αυτή την ρύθμιση, όλα τα αποκρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου απεικονίζονται στο παράθυρο του Secure Viewer μαζί με μια ειδική TEMPEST γραμματοσειρά προστασίας από εισβολή και έτσι δεν μπορούν να σωθούν σε αποκρυπτογραφημένη μορφή.
- **Word wrap clear-signed messages at column [ ]:** Αυτή η ρύθμιση προσδιορίζει τον αριθμό των στηλών όπου μία αυστηρή επιστροφή μεταφοράς (carriage return) χρησιμοποιείται για να παγιδεύσει το κείμενο στην ψηφιακή μας υπογραφή στην επόμενη γραμμή. Αυτό το χαρακτηριστικό είναι απαραίτητο διότι δεν χειρίζονται όλες οι εφαρμογές με τον ίδιο τρόπο την παγίδευση λέξης, το οποίο μπορεί να προξενήσει σπάσιμο στις γραμμές μέσα στα ψηφιακά υπογεγραμμένα μηνύματά μας με τέτοιο τρόπο που να μην είναι εύκολα αναγνώσιμα. Η προκαθορισμένη ρύθμιση είναι 70 στήλες η οποία ανταποκρίνεται σε προβλήματα στις περισσότερες εφαρμογές.

Σημείωση: Αν αλλάξουμε την προκαθορισμένη ρύθμιση της παγίδευσης λέξης στο PGP πρέπει να βεβαιωθούμε ότι η τιμή της είναι μικρότερη από την αντίστοιχη ρύθμιση στην εφαρμογή του ηλεκτρονικού ταχυδρομείου. Αν δώσουμε τιμή ίση ή μεγαλύτερη, carriage returns μπορεί να καταλήξει σε σπάσιμο της ψηφιακής μας υπογραφής.

Πατάμε **OK** για να σωθούν οι αλλαγές μας.

4.5.4 Ρυθμίζοντας επιλογές ισχυρών πλήκτρων

Πατάμε την καρτέλα **HotKeys** για καθορίσουμε συντομεύσεις από πατήματα πλήκτρων για λειτουργίες του PGP.



Σχήμα 39: Επιλογές ισχυρών πλήκτρων του PGP.

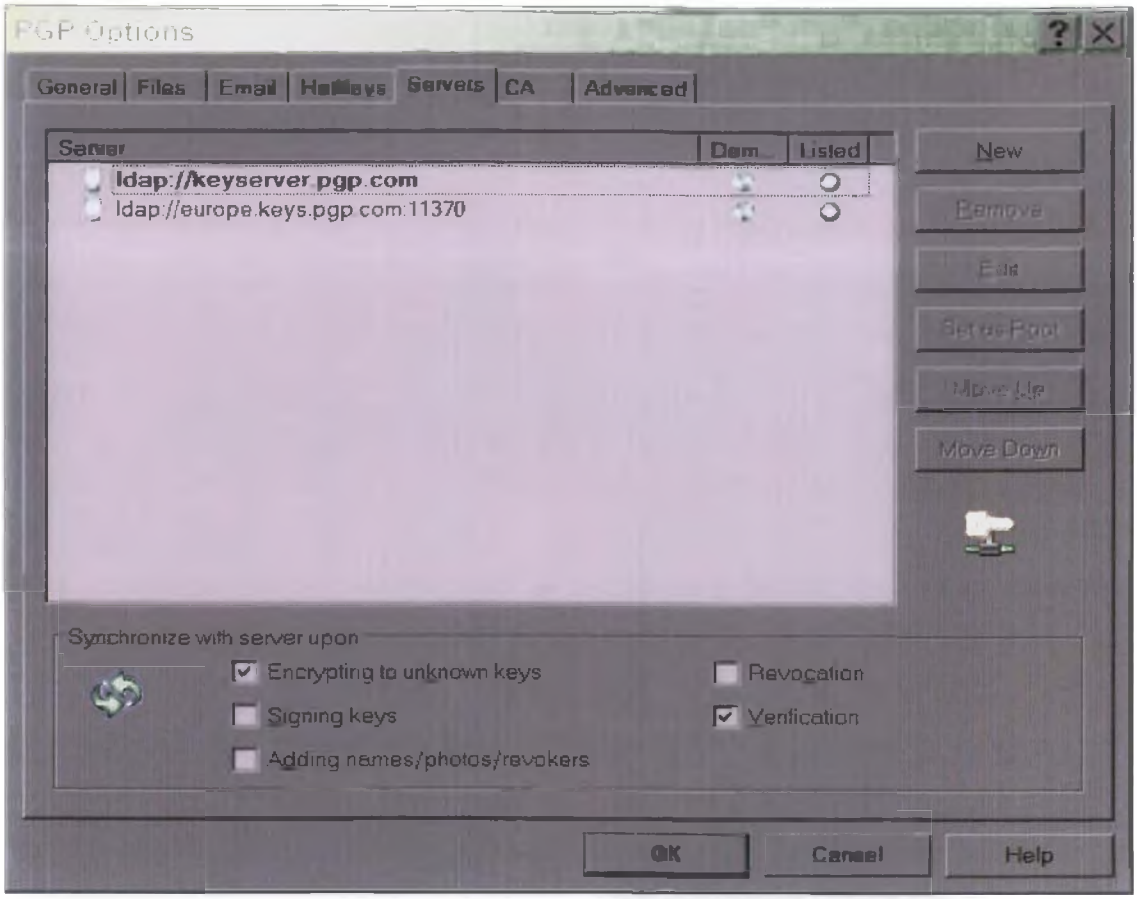
Κάνουμε τις επιλογές μας για τις ακόλουθες δυνατότητες:

- Καθαρισμός της κρύπτης της κωδικής φράσης: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-F12.
- Unmount all PGPdisks: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-Shift-U.
- Κρυπτογράφηση τρέχοντος παραθύρου: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-Shift-E.
- Υπογραφή τρέχοντος παραθύρου: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-Shift-S.
- Κρυπτογράφηση και υπογραφή τρέχοντος παραθύρου: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-Shift-C.
- Αποκρυπτογράφηση και επικύρωση τρέχοντος παραθύρου: Το προκαθορισμένο ισχυρό πλήκτρο είναι το Ctrl-Shift-D.

Πατάμε **OK** για να αποθηκευτούν οι αλλαγές.

4.5.5 Ρυθμίζοντας τα χαρακτηριστικά του εξυπηρέτη

Πατάμε την καρτέλα **Servers** για να καθορίσουμε ρυθμίσεις για εξυπηρέτες δημοσίων κλειδιών και εξυπηρέτες καταλόγων που τους χρησιμοποιούμε για να στείλουμε και να ανακτήσουμε δημόσια κλειδιά με τα οποία θα συγχρονίσουμε αυτόματα κλειδιά.



Σχήμα 40: Επιλογές εξυπηρέτη του PGP.

Το κουτί στην κορυφή της οθόνης δείχνει τους διαμορφωμένους εξυπηρέτες. Το πώς μετατρέπουμε την λίστα των εξυπηρετών και πως προσθέτουμε και τυπώνουμε την λίστα, περιγράφεται παρακάτω.

Κάνουμε τις επιλογές μας στις παρακάτω δυνατότητες:

- Κρυπτογράφηση σε άγνωστα κλειδιά: Ενεργοποιούμε αυτή την επιλογή για να έχουμε αυτόματη ενημέρωση από το PGP για άγνωστους παραλήπτες στον εξυπηρέτη και τοποθετεί αυτούς τους χρήστες που δεν υπάρχουν στη λίστα κλειδιών κατά την κρυπτογράφηση του μηνύματος ηλεκτρονικού ταχυδρομείου.
- Υπογραφή κλειδιών: Ενεργοποιούμε αυτή την επιλογή για να επιτρέψουμε σε κλειδιά τα οποία πρώτα έχουμε υπογράψει να αναβαθμιστούν από τον εξυπηρέτη και στη συνέχεια οι αλλαγές να σταλλούν στον εξυπηρέτη με την ολοκλήρωση της αναβάθμισης.
- Προθήκη ονομάτων/φωτογραφιών/ακυρώσεις: Ενεργοποιούμε αυτή την επιλογή για να επιτρέψουμε σε κλειδιά στα οποία έχουν προστεθεί ονόματα, φωτογραφίες, ή ακυρώσεις, αρχικά να αναβαθμιστούν από τον εξυπηρέτη και στη συνέχεια οι αλλαγές μας να σταλλούν στον εξυπηρέτη με την ολοκλήρωση της αναβάθμισης. Αναβαθμίζοντας το κλειδί πριν εξασφαλίσουμε ότι, για παράδειγμα, το κλειδί δεν έχει ακυρωθεί πριν την τελευταία αναβάθμισή του.
- Ακύρωση: Ενεργοποιούμε αυτή την επιλογή για να επιτρέψουμε σε κλειδιά στα οποία έχουν ακυρωθεί, αρχικά να αναβαθμιστούν από τον εξυπηρέτη και στη συνέχεια οι αλλαγές μας να σταλλούν στον εξυπηρέτη με την ολοκλήρωση της αναβάθμισης.
- Επικύρωση: Ενεργοποιούμε αυτή την επιλογή, για να έχουμε αυτόματη αναζήτηση και εισαγωγή από τον εξυπηρέτη κλειδιών όταν επικυρώνουμε ένα υπογεγραμμένο μήνυμα ή αρχείο ηλεκτρονικού ταχυδρομείου για το οποίο δεν κατέχουμε το δημόσιο κλειδί του

αποστολέα.

4.5.5.1 Μετατρέποντας τη λίστα εξυπηρετών

Τα κουμπιά στη δεξιά πλευρά της λίστας εξυπηρετών μας επιτρέπουν να την μετατρέψουμε:

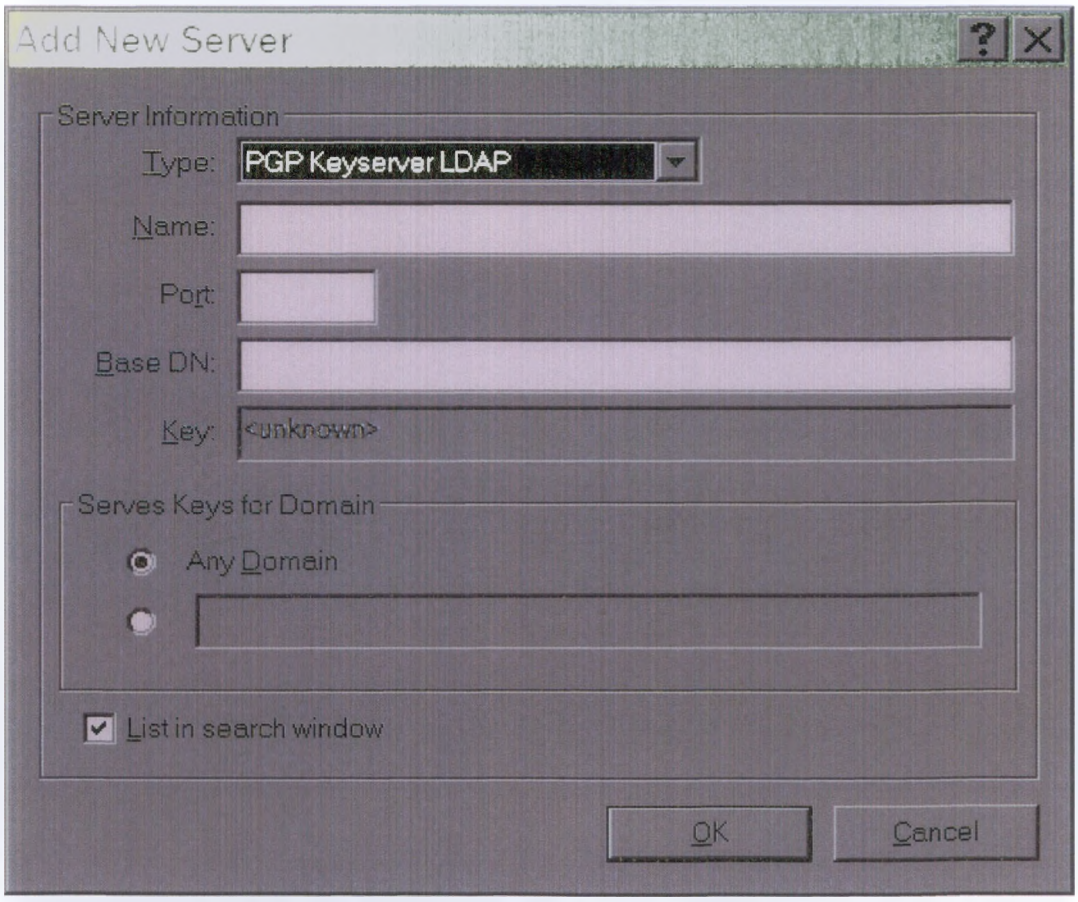
- **New:** Προσθέτει έναν καινούριο εξυπηρέτη στην λίστα
- **Remove:** Αφαιρεί τον επιλεγμένο εξυπηρέτη από την λίστα
- **Edit:** Επιτρέπει να γράψουμε πληροφοριακά στοιχεία για τοβν επιλεγμένο εξυπηρέτη
- **Set As Root:** Αναγνωρίζει τον εξυπηρέτη εκκίνησης που χρησιμοποιήθηκε για εταιρικές λειτουργίες, όπως η αναβάθμιση σε ομάδες λιστών, αποστολή σε ομάδες λίστας, αναβάθμιση συστηνόντων κ.λ.π. Στις ρυθμίσεις εταιρίας (corporate), ο διαχειριστής του PGP θα τις έχει ήδη διαμορφώσει.
- **Move Up** και **Move Down:** Χρησιμοποιούμε αυτά τα κουμπιά για να τακτοποιήσουμε τους εξυπηρέτες με τη σειρά που επιθυμούμε.

4.5.5.2 Προσθέτοντας και εγγράφοντας εξυπηρέτες

Για να προσθέσουμε έναν καινούριο εξυπηρέτη ή να τυπώσουμε έναν ήδη υπάρχον:

1. Πατάμε το κουμπί **New**. (Εάν τυπώνουμε έναν υπάρχον εξυπηρέτη, πατάμε πάνω σ' αυτόν που θέλουμε να τυπώσουμε και πατάμε **Edit**).

   Εμφανίζεται η οθόνη προσθήκης νέου εξυπηρέτη.



Σχήμα 41: Προσθήκη νέου εξυπηρέτη

2. Στο πτυσσόμενο μενού **Type,** επιλέγουμε τον τύπο του εξυπηρέτη που χρησιμοποιούμε για να προσπελάσουμε τον εξυπηρέτη κλειδιών. Οι επιλογές μας είναι:

- **HTTP** εξυπηρέτης κλειδιών PGP. Αποθήκευση και ανάκτηση κλειδιών PGP χρησιμοποιώντας εξυπηρέτη κλειδιών βασιζόμενο στο διαδίκτυο.
- **LDAP** εξυπηρέτης κλειδιών PGP. Αποθήκευση και ανάκτηση κλειδιών PGP χρησιμοποιώντας εξυπηρέτη κλειδιών μέσω των LDAP.
- **LDAPS** εξυπηρέτης κλειδιών PGP. Αποθήκευση και ανάκτηση κλειδιών PGP χρησιμοποιώντας εξυπηρέτη κλειδιών μέσω των LDAPS.
- **X.509 Directory LDAP.** Χρησιμοποιούμε αυτή την επιλογή όταν χρησιμοποιούμε γενικό Εξυπηρέτη κατηγορίας LDAP για αποθήκευση και ανάκτηση πιστοποιήσεων X.509 που περιέχεται σε iPlanet CMS ή υπηρεσίες πιστοποίησης της Microsoft.
- **X.509 Directory LDAPS**. Χρησιμοποιούμε αυτή την επιλογή όταν χρησιμοποιούμε γενικό Εξυπηρέτη κατηγορίας LDAPS για αποθήκευση και ανάκτηση πιστοποιήσεων X.509 που περιέχεται σε iPlanet CMS ή υπηρεσίες πιστοποίησης της Microsoft.

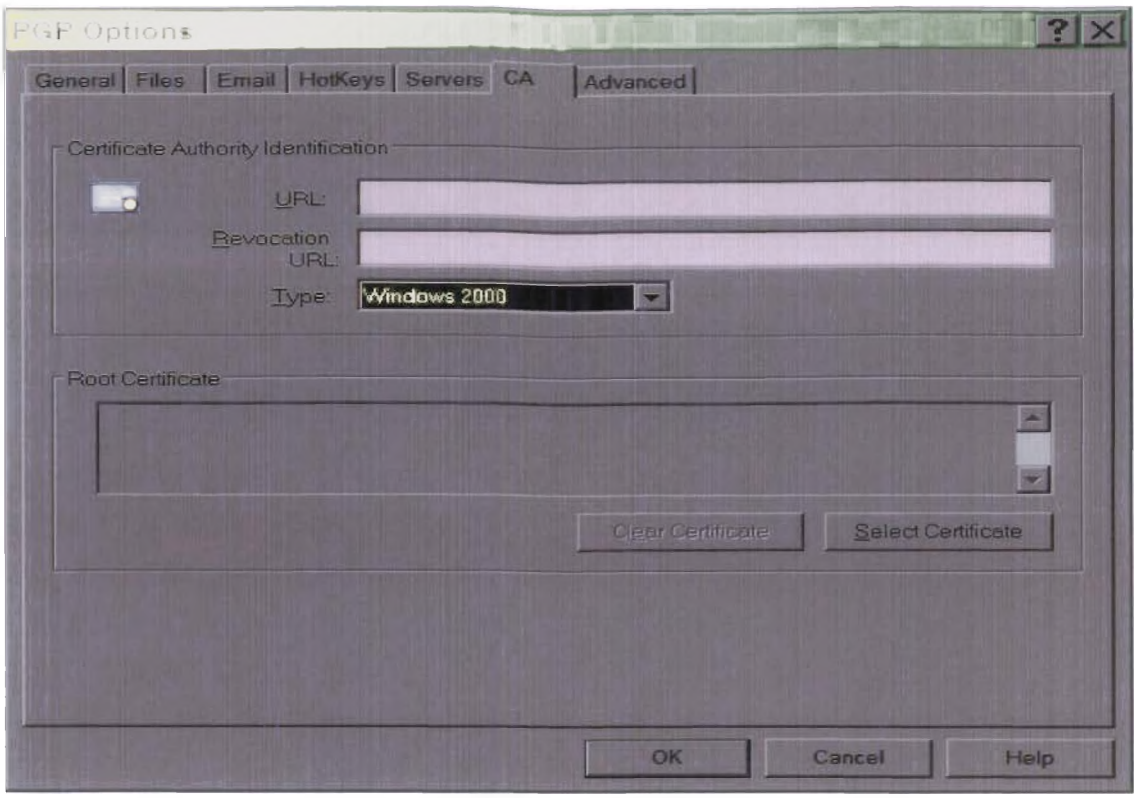
3. Στο κουτί **Name**, εισάγουμε το κύριο όνομα της διεύθυνσης IP του εξυπηρέτη. Για παράδειγμα server.pgp.com ή 123.45.67.89
4. Στο κουτί **Port**, εισάγουμε τον αριθμό της θύρας του εξυπηρέτη. Για παράδειγμα 11371 χρησιμοποιείται για πεπαλαιωμένο τύπο HTTP εξυπηρέτη κλειδιών, 389 για LDAP εξυπηρέτες κλειδιών. Αν δεν γνωρίζουμε τον αριθμό της θύρας, αφήνουμε κενό αυτό το κουτί. Θα χρησιμοποιηθεί ο προκαθορισμένος αριθμός της θύρας του εξυπηρέτη που έχουμε διαμορφώσει.
5. Το κουτί **Key** αφορά τους εξυπηρέτες LDAPS. Ο εξυπηρέτης κλειδιού χρησιμοποιείται από τον εξυπηρέτη για πιστοποίηση της σύνδεσης. (Δεν εμφανίζεται ενημέρωση για το κλειδί μέχρι να συνδεθούμε με τον εξυπηρέτη).
6. Στο **Servers Key for Domain** επιλέγουμε **Any Domain** για να επιτρέψουμε στο PGP να στείλει κλειδιά από κάθε κύριο, σε αυτόν τον εξυπηρέτη κλειδιών. Αυτή η επιλογή εφαρμόζει επίσης και αυτόματες αναζητήσεις και αναβαθμίσεις. Είναι προκαθορισμένα ενεργοποιημένη. Αν θέλουμε το PGP να στέλνει μόνο κλειδιά από έναν κύριο σε αυτόν τον εξυπηρέτη κλειδιών, επιλέγουμε **Any Domain**. Τότε εισάγουμε το όνομα του κύριου στον χώρο που διατίθεται. Για παράδειγμα, αν καθορίσουμε τον κύριο pgp.com, μόνο τα κλειδιά των οποίων η διεύθυνση καταλήγει σε pgp.com θα σταλούν σε αυτόν τον εξυπηρέτη.
7. Μαρκάρουμε το κουτάκι **List in search window**, αν θέλουμε αυτός ο εξυπηρέτης κλειδιών να προστεθεί στην λίστα στο παράθυρο αναζήτησης κλειδιών PGP.
8. Όταν έχουμε κάνει τις επιλογές μας πατάμε **OK**.

   Η οθόνη πληροφόρησης εξυπηρέτη εξαφανίζεται και ο εξυπηρέτης που μόλις διαμορφώσαμε απεικονίζεται μέσα στην λίστα.

9. Πατάμε **OK** για να σώσουμε τις αλλαγές.

4.5.6 Ρυθμίζοντας επιλογές πιστοποίησης αυθεντικότητας (Certificate Authority CA)

Χρησιμοποιούμε την καρτέλα CA για να προσθέσουμε την πιστοποίηση X.509 στο κλειδί PGP. Πριν την προσθήκη θα πρέπει αρχικά να καθορίσουμε αρχική πιστοποίηση CA από τον εξυπηρέτη κλειδιών της εταιρίας μας.

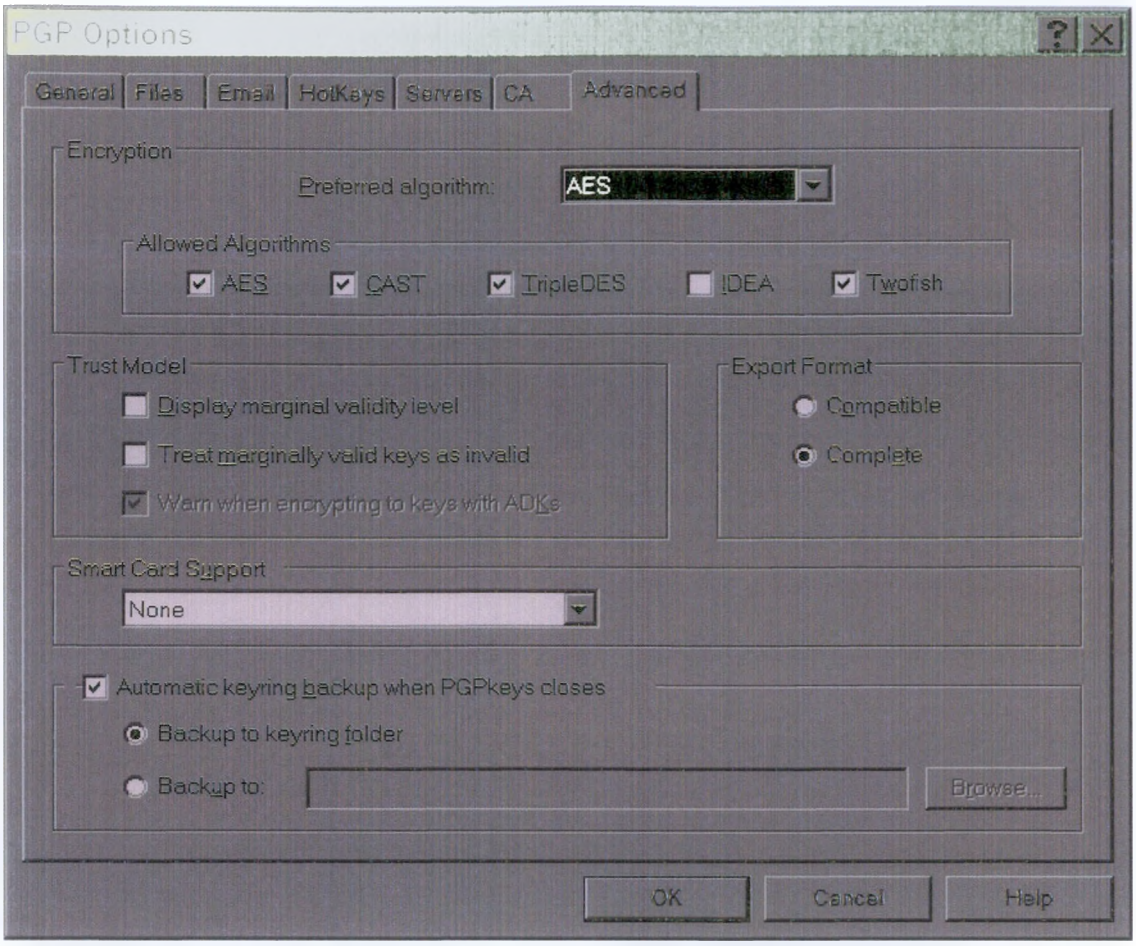


Σχήμα 42: Επιλογές πιστοποίησης αυθεντικότητας του PGP.

Πατάμε OK για να σώσουμε τις αλλαγές.

4.5.7 Ρυθμίζοντας προηγμένες επιλογές

Χρησιμοποιούμε την καρτέλα **Advanced** για να επιλέξουμε τους προτιμόμενους κρυπτογραφικούς αλγόριθμους, τους επιτρεπόμενους αλγόριθμους, επιλογές εμπιστευτικότητας κλειδιών, μορφοποίηση εξερχόμενων κλειδιών και ρυθμίσεις αυτόματου backup λίστας κλειδιών.



Σχήμα 43: Προηγμένες επιλογές του PGP.

Κάνουμε τις επιλογές μας στις παρακάτω δυνατότητες:

- **Preferred Algorithm**. Επιλέγουμε τον προτιμώμενο αλγόριθμο. Οι επιλογές είναι:

  i. **AES**: Είναι η προκαθορισμένη επιλογή. Ο αναβαθμισμένος αλγόριθμος Advanced Encryption Standard(AES) είναι επιλεγμένος από το διεθνές ινστιτούτο Προτύπων και Τεχνολογίας (NIST-National Institute of Standards and Technology) και περιέχει το μπλοκ κρυπτογραφήματος Rijndael σχεδιασμένο από τους Joan Daemen και Vincent Rijmen. Έχει μελετηθεί έτσι ώστε να είναι ταχύτερος και μικρότερος από τους ανταγωνιστικούς του αλγόριθμους. Αυτή η επιλογή επιτρέπει στο PGP να χρησιμοποιεί κλειδιά και μπλοκ μεγεθών 256, 192 και 128 bits.

  ii. **CAST**: Είναι ένα 128-bit κρυπτογράφημα. Είναι ισχυρός αλγόριθμος κρυπτογράφησης και χρησιμοποιείται σε στρατιωτικές εφαρμογές. Έχει την φήμη της καλής αντίστασης σε μη εξουσιοδοτημένη χρήση.

  iii. **TripleDes**: Είναι αλγόριθμος της κυβέρνησης των Η.Π.Α. και αποδείχθηκε ασυναγώνιστος σε χρονικές δοκιμές. Είναι μια μορφή κρυπτογράφησης στην οποία ο αλγόριθμος DES χρησιμοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά. (Αν θέλουμε να χρησιμοποιήσουμε τον TripleDes, πρέπει να τον επιλέξουμε πριν την παραγωγή των κλειδιών).

  iv. **IDEA**: Είναι ένας αλγόριθμος που χρησιμοποιείται για όλα τα κλειδιά που εξάγονται από τον RSA μέσω του PGP. (Αν πρόκειτε να χρησιμοποιήσουμε τον IDEA, πρέπει να τον επιλέξουμε πριν την παραγωγή των κλειδιών).

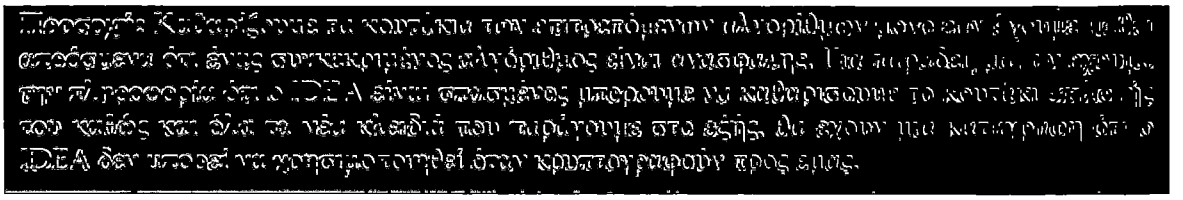
  v. **Twofish**: Είναι ένας συμμετρικός αλγόριθμος με 256-bit μπλοκ κρυπτογράφησης. Είναι ένας από τους πέντε αλγόριθμους που επέλεξε το διεθνές ινστιτούτο

Προτύπων και Τεχνολογίας (NIST-National Institute of Standards and Technology) και συναγωνίστηκαν τον Advanced Encryption Standard (AES).

Οι αλγόριθμοι προτίμησης επιδρούν επιλεκτικά στην διαδικασία ως εξής:

- Όταν χρησιμοποιούμε συμβατική κρυπτογράφηση, το προτιμώμενο κρυπτογράφημα χρησιμοποιείται για κρυπτογράφηση.
- Όταν δημιουργούμε ένα κλειδί, το προτιμώμενο κρυπτογράφημα καταγράφεται ως τμήμα του κλειδιού έτσι ώστε άλλα άτομα θα χρησιμοποιήσουν αυτόν τον αλγόριθμο όταν κρυπτογραφούν σε εμάς.

- **Allowed Algorithms**: είναι καταγεγραμμένοι ως τμήμα του κλειδιού έτσι που άλλα άτομα θα χρησιμοποιήσουν έναν από αυτούς τους αλγόριθμους όταν κρυπτογραφούν σε εμάς εάν ο προτιμώμενος αλγόριθμος δεν είναι διαθέσιμος σε αυτούς.



Η κρυπτογράφηση σε ένα δημόσιο κλειδί θα αποτύχει, αν τόσο οι προτιμώμενοι αλγόριθμοι όσο και και κάθε ένας από τους επιτρεπόμενους αλγόριθμους, δεν είναι διαθέσιμοι στο άτομο που κρυπτογραφούμε το μήνυμα.

- Display marginal validity level: Χρησιμοποιούμε αυτό το κουτί ελέγχου για να καθορίσουμε πότε θα απεικονίζεται πληροφορία για κλειδιά οριακά έγκυρα, ή απλά θα δείχνει την εγκυρότητα ως ενεργή ή ανενεργή (on/off). Η οριακή εγκυρότητα εμφανίζεται ως μπάρα από εικονίδια με διαφορετικής σκίασης μοτίβο. Η τύπος on/off εγκυρότητας εμφανίζεται σε κυκλικά εικονίδια. Πράσινο για έγκυρο, γκρι για άκυρο (κλειδί που δεν έχει τύπο εγκυρότητας, προφανώς δεν έχει υπογραφεί από κάποιον έμπιστο συστάτη ή από εμάς).
- Treat marginally valid keys as invalid: Χρησιμοποιούμε αυτό το κουτί ελέγχου για να καθορίσουμε πότε να μεταχειριστούμε όλα τα οριακά έγκυρα κλειδιά ως άκυρα. Με την ενεργοποίηση αυτής της επιλογής προκύπτει ένα πλαίσιο διαλόγου επιλογής κλειδιού που εμφανίζεται κάθε φορά που κρυπτογραφούμε σε οριακής εγκυρότητας κλειδιά.
- Warn when encrypting to keys with ADKs: Χρησιμοποιούμε αυτό το κουτί ελέγχου για να καθορίσουμε πότε να εκδόσουμε μία προειδοποίηση κάθε φορά που μια κρυπτογράφηση σε κλειδί σχετίζεται με μια επιπρόσθετη αποκρυπτογράφηση κλειδιού.
- Export Format: Οι επιλογές είναι:
  - **Compatible:** εξάγει κλειδιά σε μορφοποίηση συμβατή με προηγούμενες εκδόσεις του PGP.
  - **Complete:** εξάγει την νέα μορφοποίηση κλειδιού, η οποία περιλαμβάνει φωτογραφική αναγνώριση και πιστοποίηση X.509.
- Smart card support: Επιλέγουμε τον τύπο της έξυπνης κάρτας που θέλουμε να υποστηρίζει το PGP. Μπορεί να υποστηρίζει μόνο ένα τύπο κάρτας για κάθε δεδομένη στιγμή. Οι επιλογές είναι:
  - **None:** Όταν δεν θέλουμε έναν αναγνώστη έξυπνης κάρτας εγκατεστημένο ή δεν θέλουμε το PGP να υποστηρίζει κάποιον τύπο έξυπνης κάρτας.
  - **Aladdin:** Όταν θέλουμε να χρησιμοποιούμε το Aladdin eToken Pro product line του

USB έξυπνης κάρτας μαζί με το PGP.

- **Gemplus:** Όταν θέλουμε να χρησιμοποιούμε το προϊόν GemPlus GemSafe Enterprise έξυπνης κάρτας, μαζί με το PGP.
- **Rainbow:** Όταν θέλουμε να χρησιμοποιούμε το προϊόν Rainbow iKey 20XX έξυπνης κάρτας, μαζί με το PGP.
- **Schlumberger:** Όταν θέλουμε να χρησιμοποιούμε το προϊόν Schlumberger Cryptoflex έξυπνης κάρτας, μαζί με το PGP.
- **Other:** Αν θέλουμε να χρησιμοποιήσουμε έναν άλλον τύπο έξυπνης κάρτας διαφορετικό από τους προαναφερόμενους. Θα ερωτηθούμε να εισάγουμε το όνομα αρχείου για το DLL για την κάρτα που θέλουμε να υποστηρίζει το PGP.

- **Automatic keyring backup when PGPkeys closes:** Επιλέγουμε αυτό το κουτί ελέγχου για να δημιουργήσουμε ένα εφεδρικό αντίγραφο στις λίστες δημοσίων και ιδιωτικών κλειδιών, αυτόματα μόλις κλείνουμε το PGP.
  - **Back up to keyring folder:** Για να αποθηκεύσουμε τα εφεδρικά αρχεία λίστας κλειδιών μέσα στον προκαθορισμένο φάκελο λίστας κλειδιών του PGP.
  - **Back up to:** Για να προσδιορίσουμε την τοποθεσία στην οποία θέλουμε να αποθηκεύσουμε τα εφεδρικά αρχεία.

Πατάμε **OK** για να σώσουμε τις αλλαγές μας.

4.5.8 Ρυθμίζοντας επιλογές δίσκου PGP

Η καρτέλα PGPdisk μας επιτρέπει να στήσουμε υπάρχοντες χώρους δίσκου.

- Allow forcible unmounting of PGPdisks with open files. Κανονικά, δεν μπορούμε να αυτόματα ένα τμήμα δίσκου PGP αν κάποιο από τα αρχεία που περιέχει είναι ανοιχτά. Μαρκάροντας αυτή την επιλογή επιτρέπουμε την αναγκαστική με ανοιχτά αρχεία.

  Η επιλογή **Don't ask before forcibly unmounting a PGPdisk**, επιτρέπει την αυτόματη αποπροσάρτηση δίσκου του PGP χωρίς αρχική προειδοποίηση για κάποια αρχεία που μπορεί να είναι ανοιχτά.

[redacted]

- Auto unmount after 15 minutes of inactivity. Όταν μαρκάρουμε αυτή την επιλογή, ο δίσκος του PGP προκαλεί την αυτόματη αποπροσάρτηση κάθε προσαρτημένου τμήματος δίσκου του PGP όταν ο υπολογιστής μας είναι σε αδράνεια για τον αριθμό των λεπτών που αναγράφεται μέσα στο κουτί. Μπορούμε να θέσουμε αυτή την τιμή από 1 εώς 999 λεπτά.

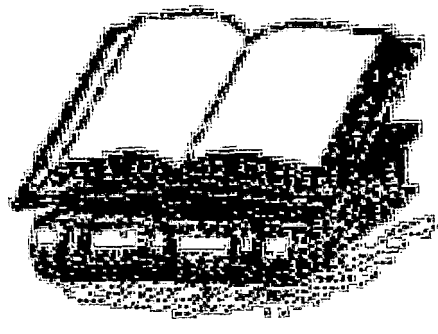
[redacted]

- Auto unmount on computer sleep. Όταν μαρκάρουμε αυτή την επιλογή ο δίσκος του PGP προκαλεί την αυτόματη αποπροσάρτηση κάθε προσαρτημένου τμήματος PGP δίσκου όταν ο υπολογιστής μας μεταβαίνει σε κατάσταση αδράνειας (Sleep mode - δεν έχουν όλοι οι τύποι υπολογιστών Κατάσταση αδράνειας).

  Μαρκάρουμε το κουτί στην επιλογή **Prevent sleep if any PGPdisk could not be unmounted** αν θέλουμε να αποτρέψουμε τον υπολογιστή μας από αδρανοποίηση, αν ένας δίσκος PGP δεν μπορεί να αποπροσαρτηθεί.

Πατάμε **OK** για να σώσουμε τις αλλαγές.

5 ΒΙΒΛΙΟΓΡΑΦΙΑ



Σχετικά με την ιστορία της κρυπτογραφίας

[Singh99] The Code Book: The evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, Simon Singh, Doubleday & Company, 1999.

[KSS96] The Codebreakers: The story of Secret Writing, David Kahn, Simon & Schuster, 1996.

[Aegean] Aegean Park Press, http://www.aegean parkpress.com.

[Cohen95] A Short History of Cryptography, Fred Cohen, http://www.all.net/books/ip/Chap2-1.html, 1995.

Τεχνικά θέματα κρυπτογραφίας

Δικτυακοί τόποι

117.http://www.thenextwave.com/page19.html

118.http://www.sci.net/cryptic/des.htm

119.http://www.faqs.org/rfcs/rfc2144.html

120.http://www.aementus.com.br/PGP/doc/idea.html

121.http://pathome.org.uk/crypt/rsa/rsa.html

122.http://www.di-mgt.com.au/rsa_alg.html

123.http://www.netip.com/articles/keith/diffie-hellman.htm

124.http://www.itl.nist.gov/fipspubs/fip180-1.htm

125.www.iacr.org

126.www.pgpi.org

127.www.nist.gov/

128.www.ietf.org/rfc/rfc2440.txt

129.www.ietf.org/rfc/rfc3156.txt

130.http://www.eskimo.com/~weidai/cryptlib.html

131.http://inf2.pira.co.uk/top031.htm

132.http://www.infosyssec.net/infosyssec/firewl.htm

133.http://www.qmw.ac.uk/~tl6345/

134.http://www.pgp.com/

135.http://www.mod.uk/careers/recruit_home.htm

136.http://www.cdt.org/policy/

137.http://www.cryptography.com/resources/papers/index.html

138.http://www.epic.org/crypto/

139. http://www.nscl.gr/greek/recruit_home.htm

140. http://www.pgp.com/about/default.asp

Άρθρα, περιοδικά, εγχειρίδια

[PGP02-1] *An Introduction to Cryptography,* PGP Corporation, 2002.

[PGP02-2] PGP 8.0 for Windows, User's Guide, PGP Corporation, 2002.

[C01] A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols, David Carts, SANS Institute, http://www.sans.org/rr/paper.php?id=751, 2001.

Ασφάλεια δικτύων

[ZCCR00] *Building Internet Firewalls,* Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper, and Deborah Russel, 2000.

[CBL94] *Firewalls and Internet Security: Repelling the Wily Hacker,* William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, http://www.wilyhacker.com, 1994.

[KPS02] *Network Security: Private Communication in a Public World*, Charles Kaufman, Radia Perlman and Mike Speciner, 2002.

[Π03] *Ασφάλεια δικτύων υπολογιστών,* Πομπόρτσης Ανδρέας, Παπαδημητρίου Γεώργιος, 2003.

[ΒΗ03] Ασφάλεια δικύων: ο απόλυτος οδηγός για την προστασία του δικτύου σας, Chris Brenton, Cameron Hunt- Εκδόσεις Μ.Γκιούρδας, 2003.

[S96] Applied Cryptography: Protocols, Algorithms and Source Code in C, Bruce Schneier, John Wiley & Sons, 1996.

[S94] PGP: Pretty Good Privacy, Simson Garfinkel, O'Reilly, 1994.

[MOV96] Handbook of Applied Cryptography, Alfred Menezes, Paul Oorschot and Scott Vanstone, CRC Press, http://cr.crashed.net/~akrowne/hac/, 1996.

[S99] Cryptography and Network Security: Principles and Practice, William Stallings, Prentice Hall, Corp., 1999.